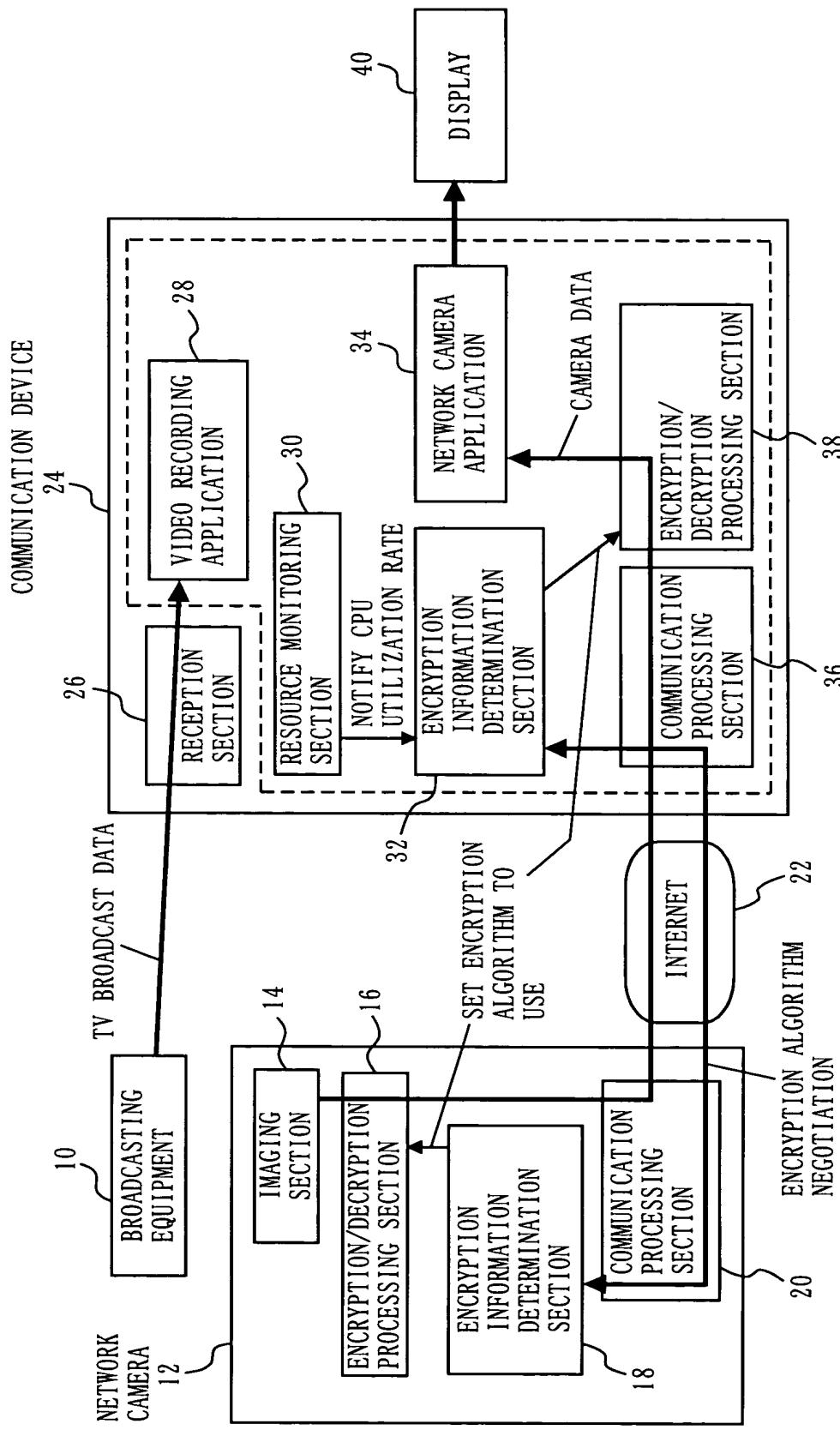


FIG. 1



38

36

22

20
ENCRYPTION ALGORITHM
NEGOTIATION

18

16

14

12

10

26

24

FIG. 2

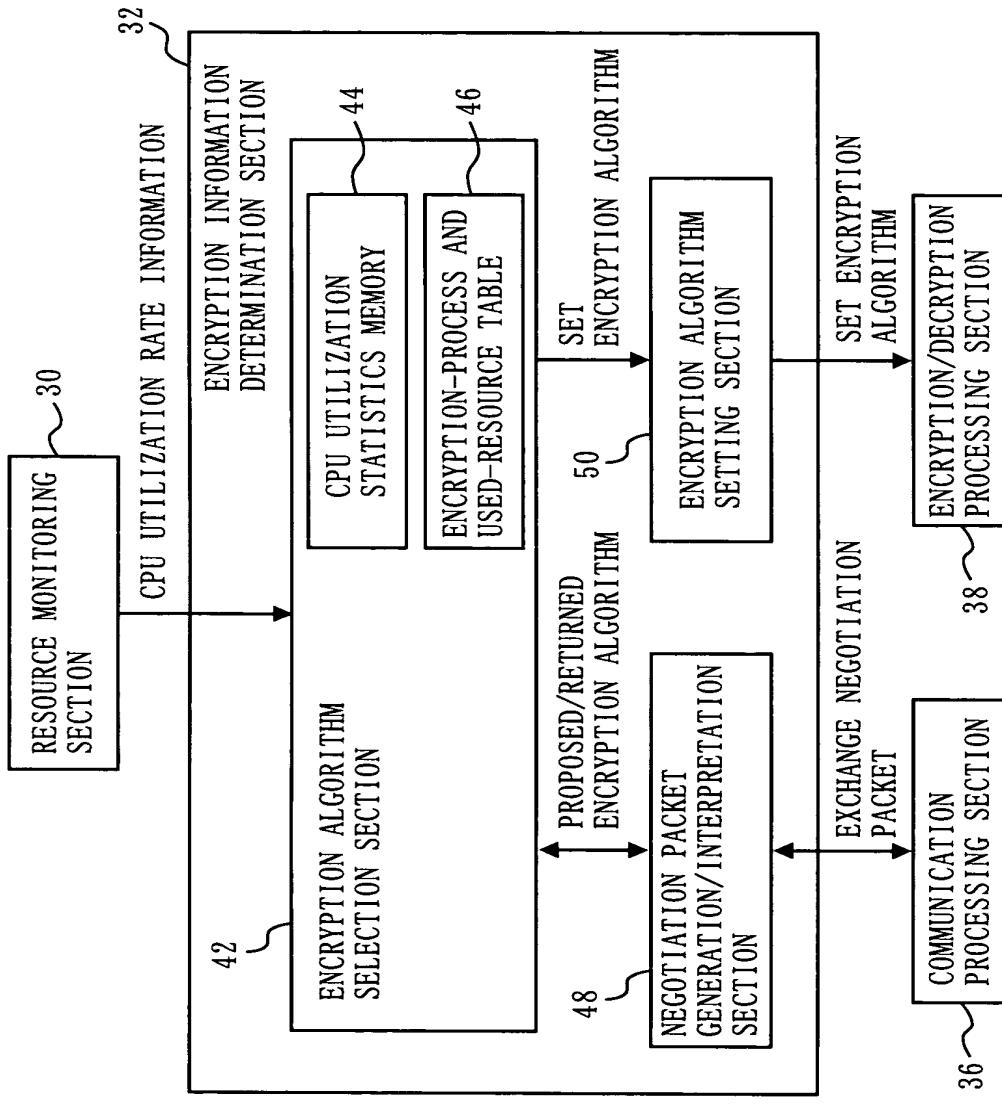
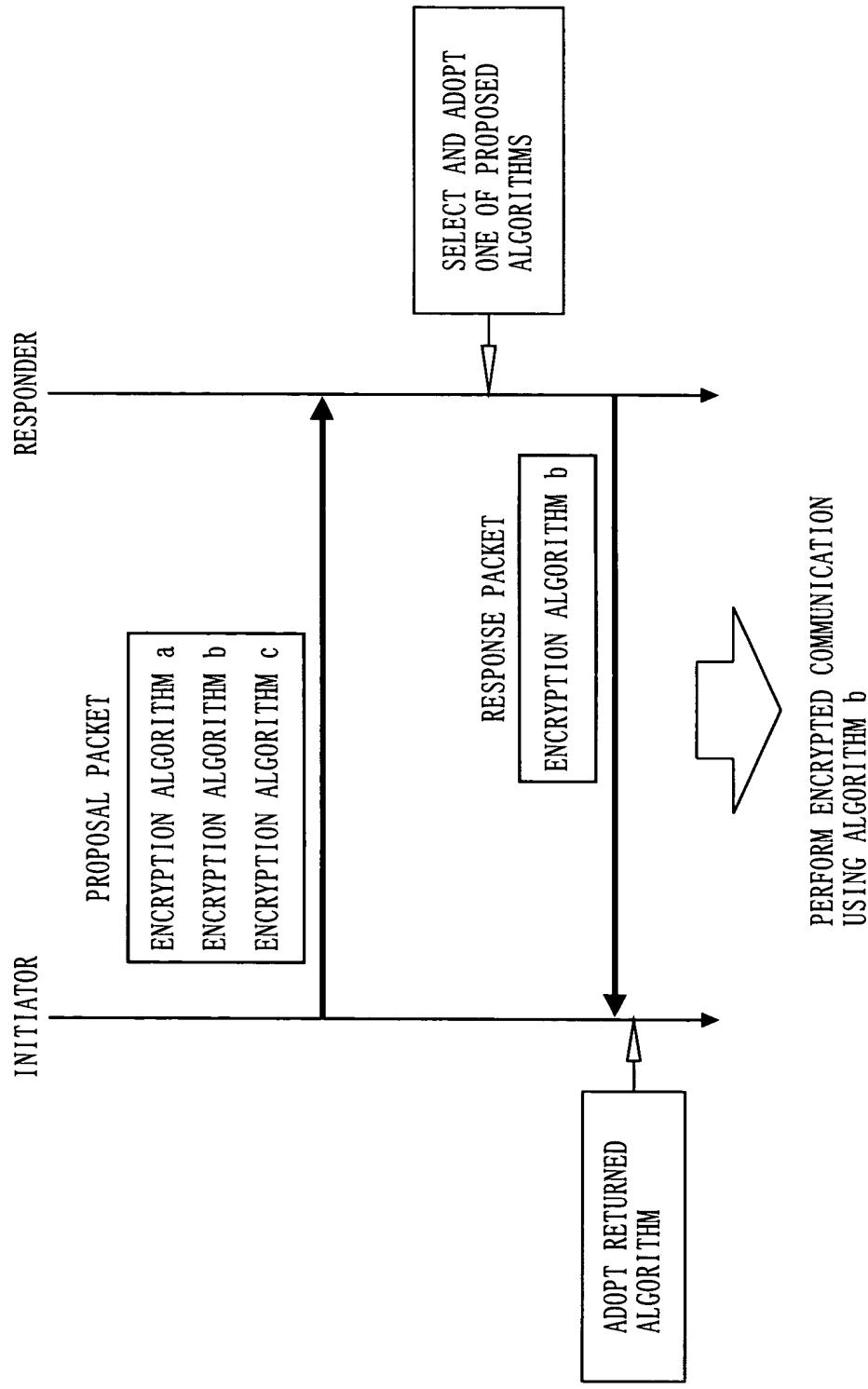
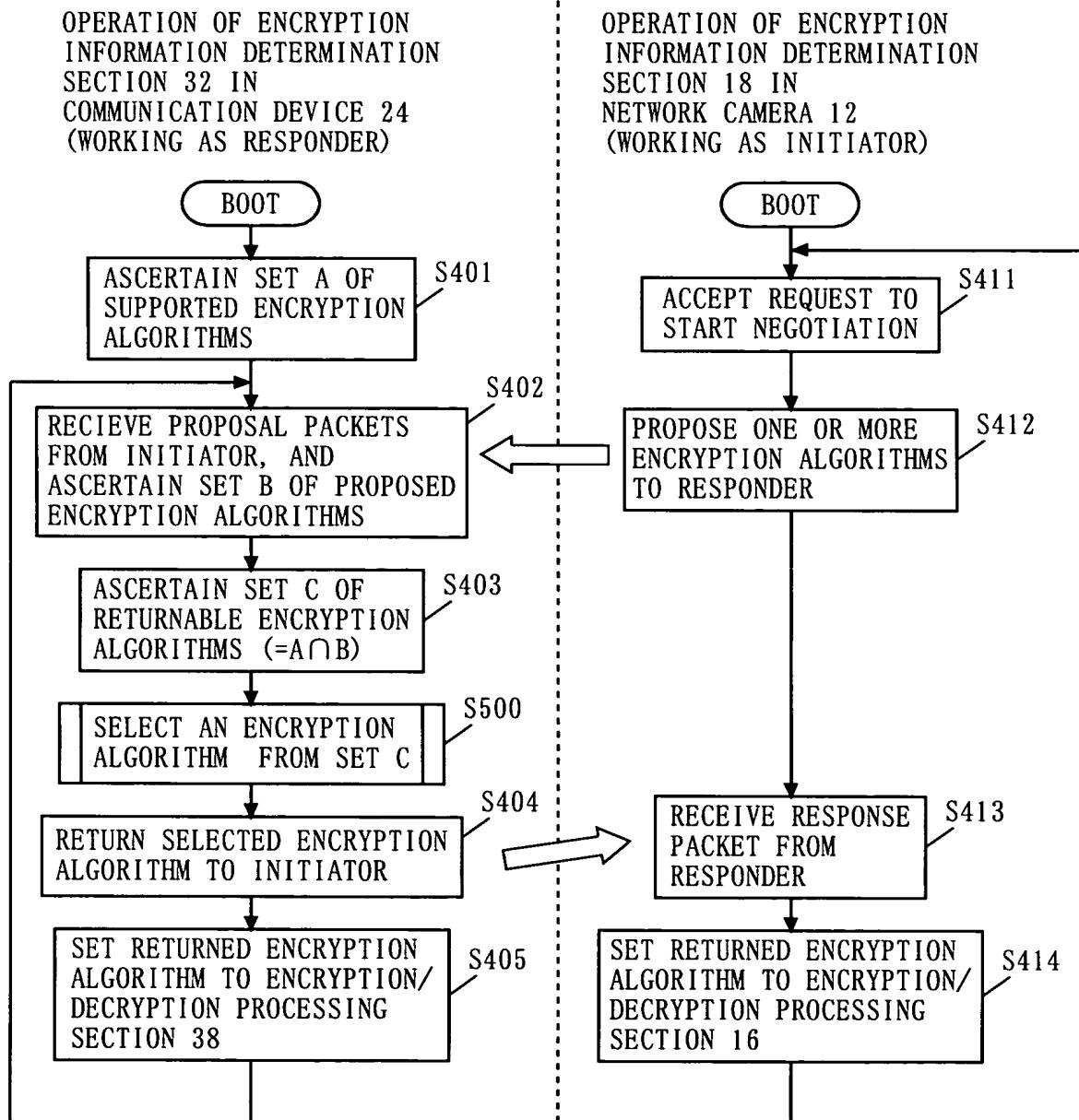


FIG. 3



F I G. 4



F I G. 5

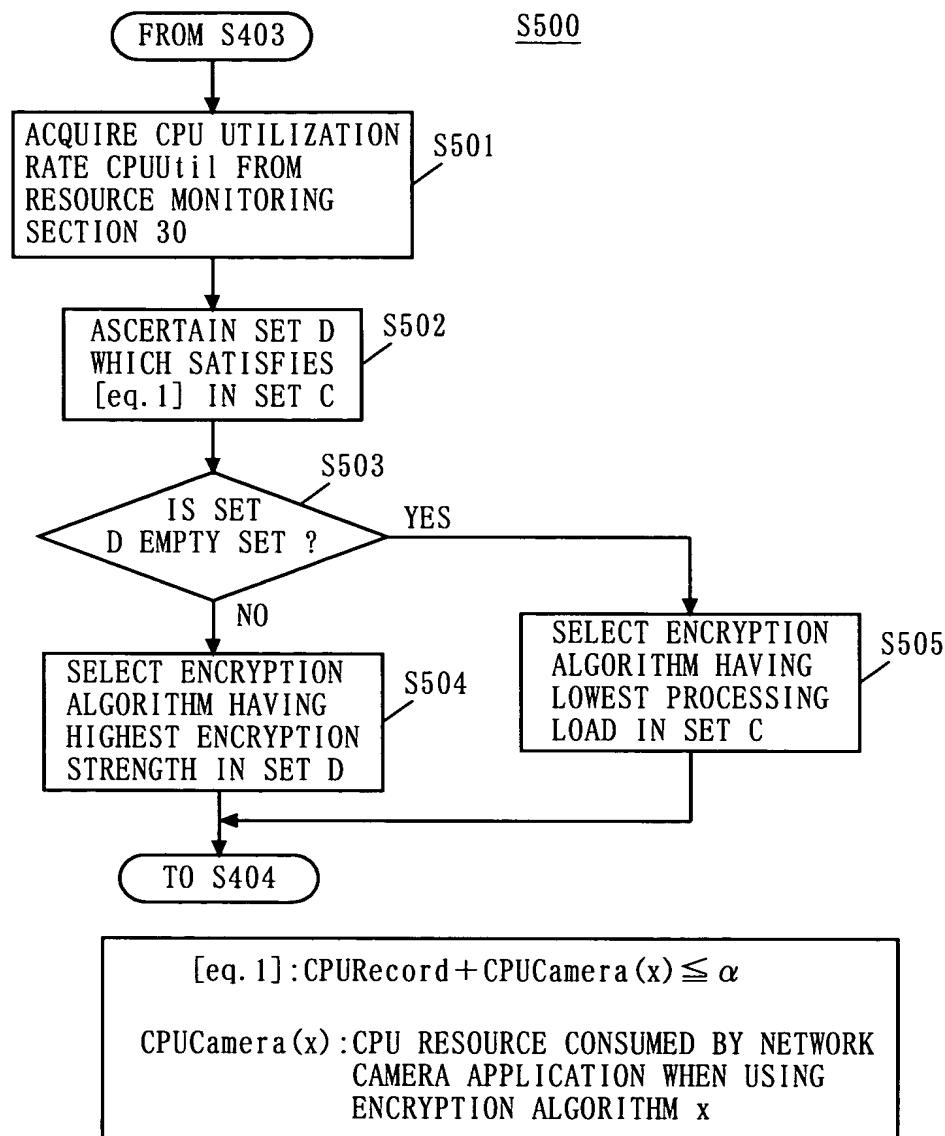
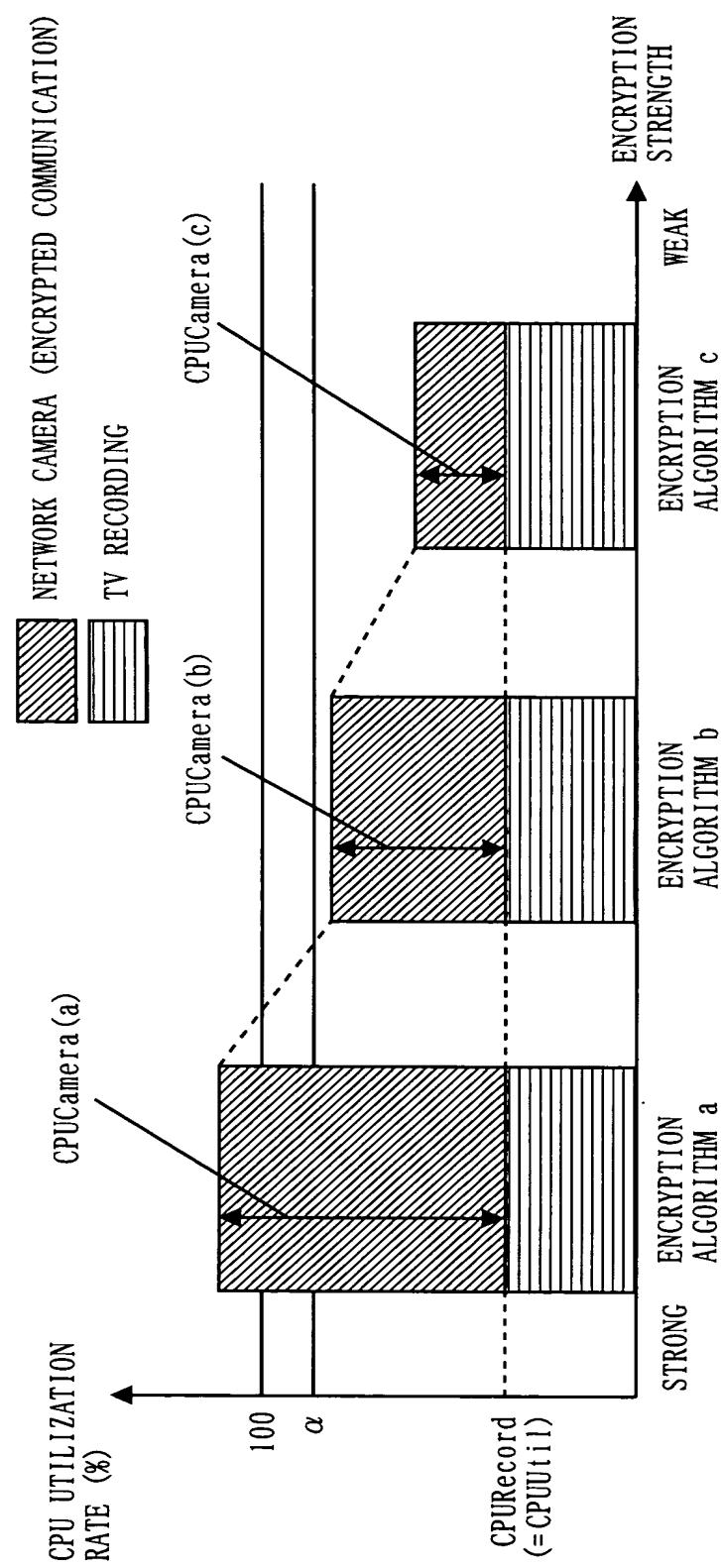


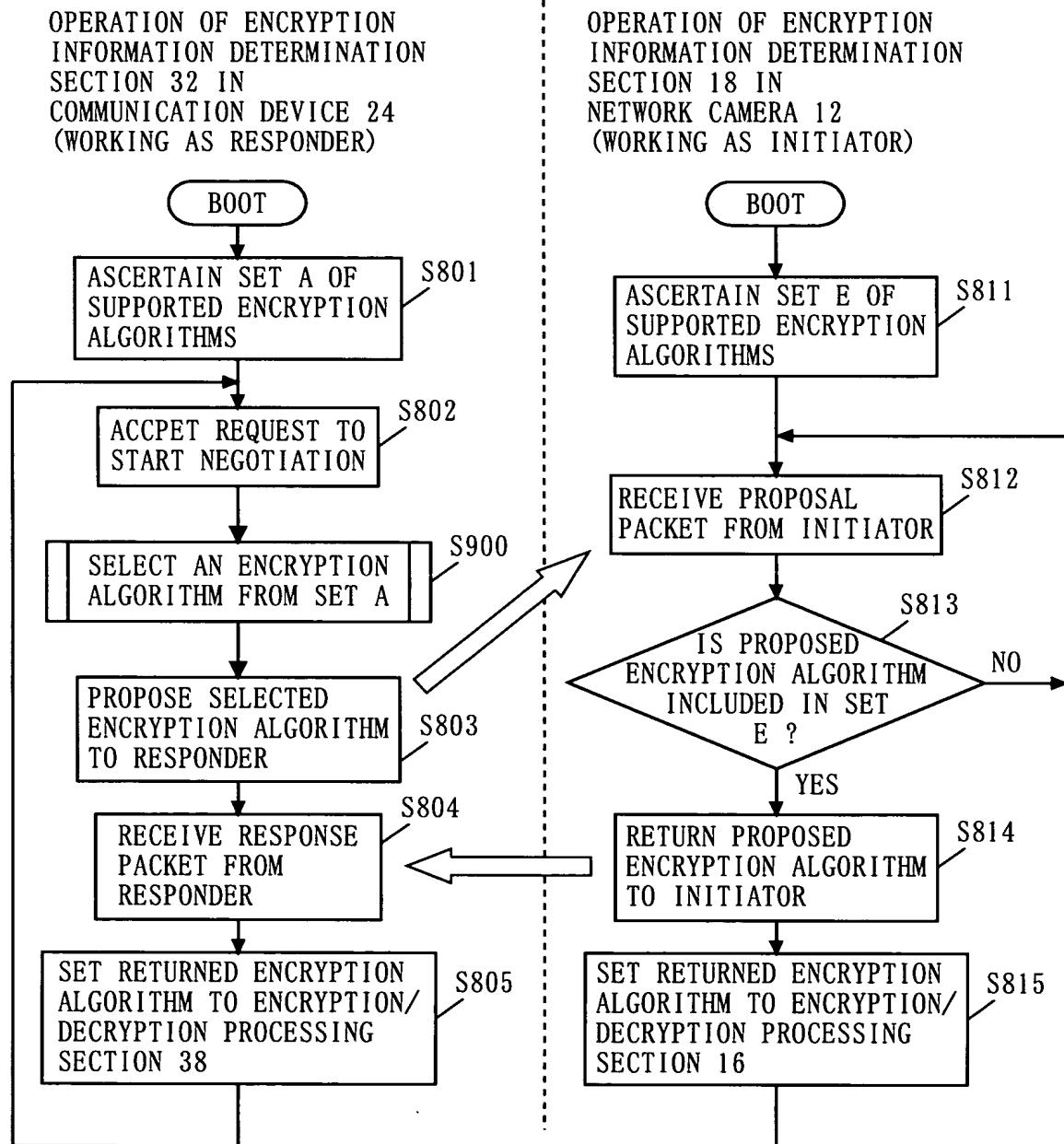
FIG. 6



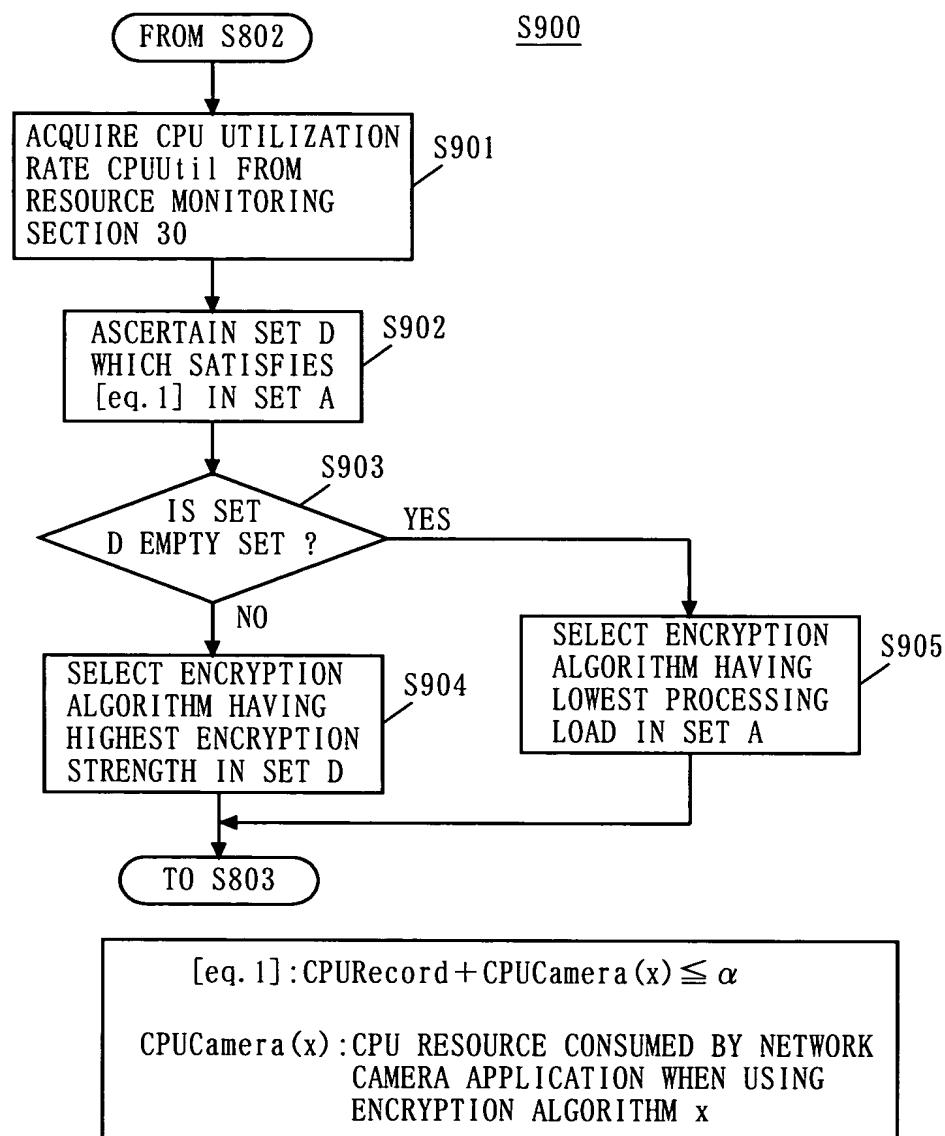
F I G. 7

ENCRYPTION ALGORITHM	EncRate()	ENCRYPTION STRENGTH
a	20	1
b	40	2
c	70	3
:	:	:

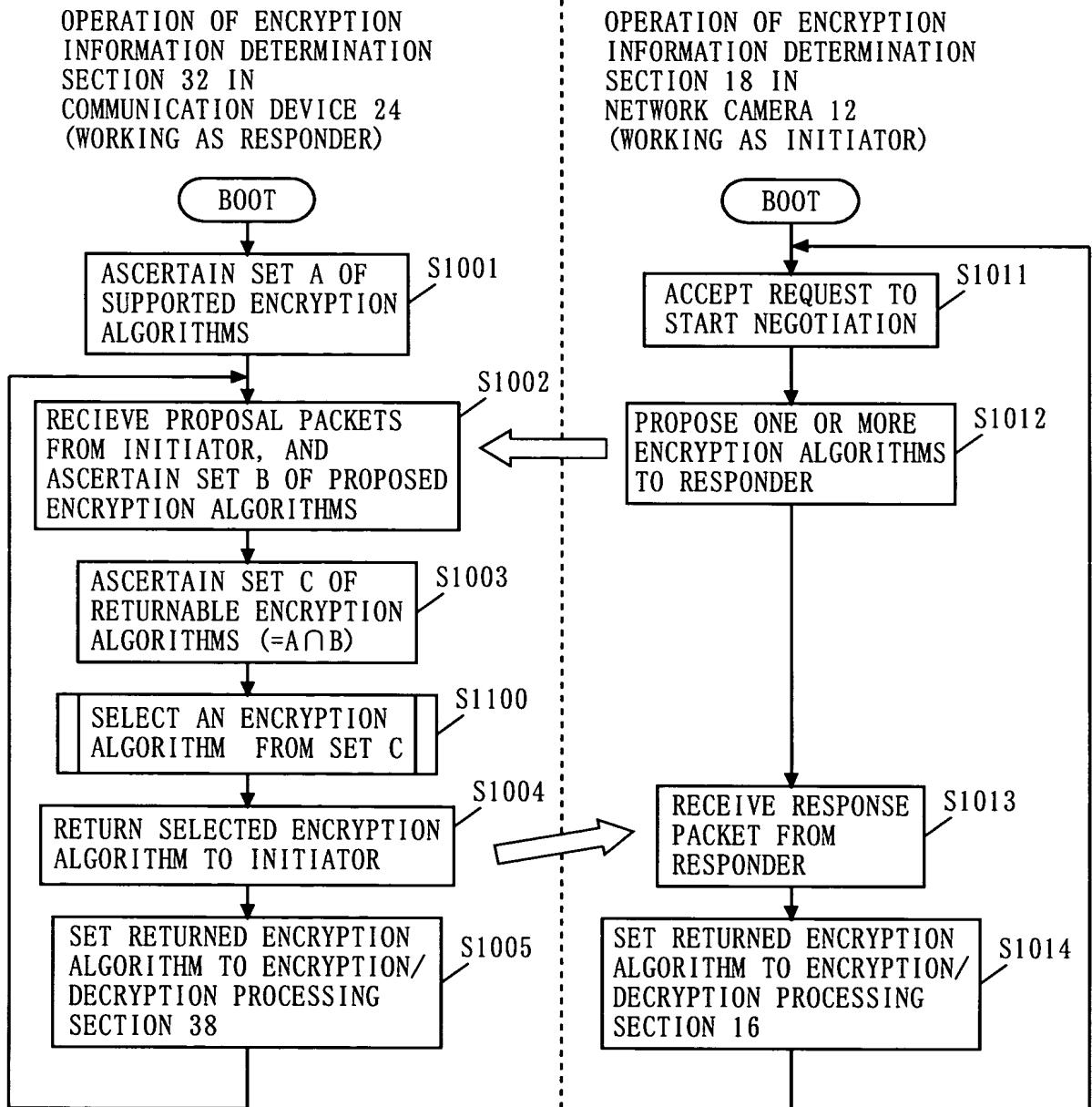
F I G. 8



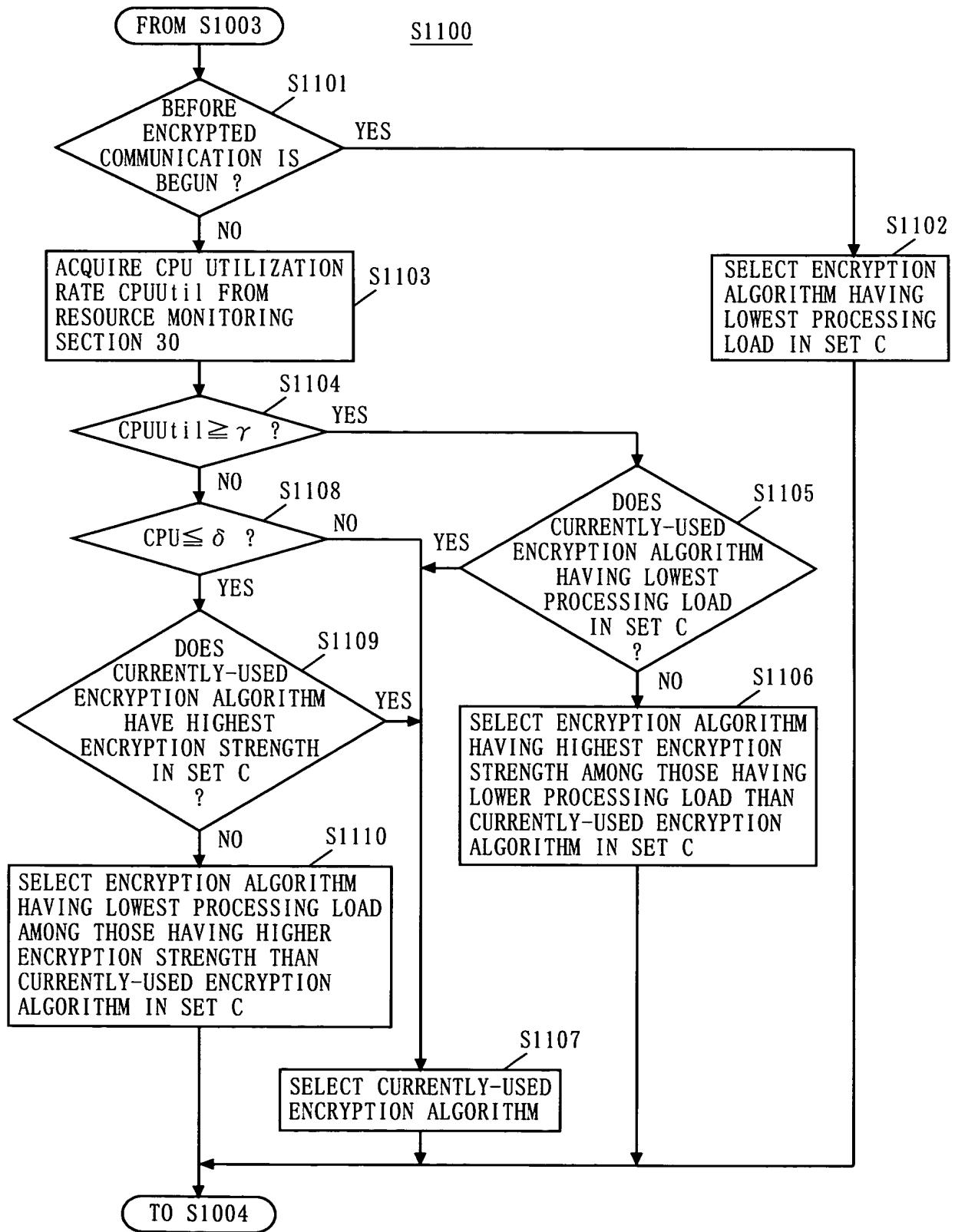
F I G. 9



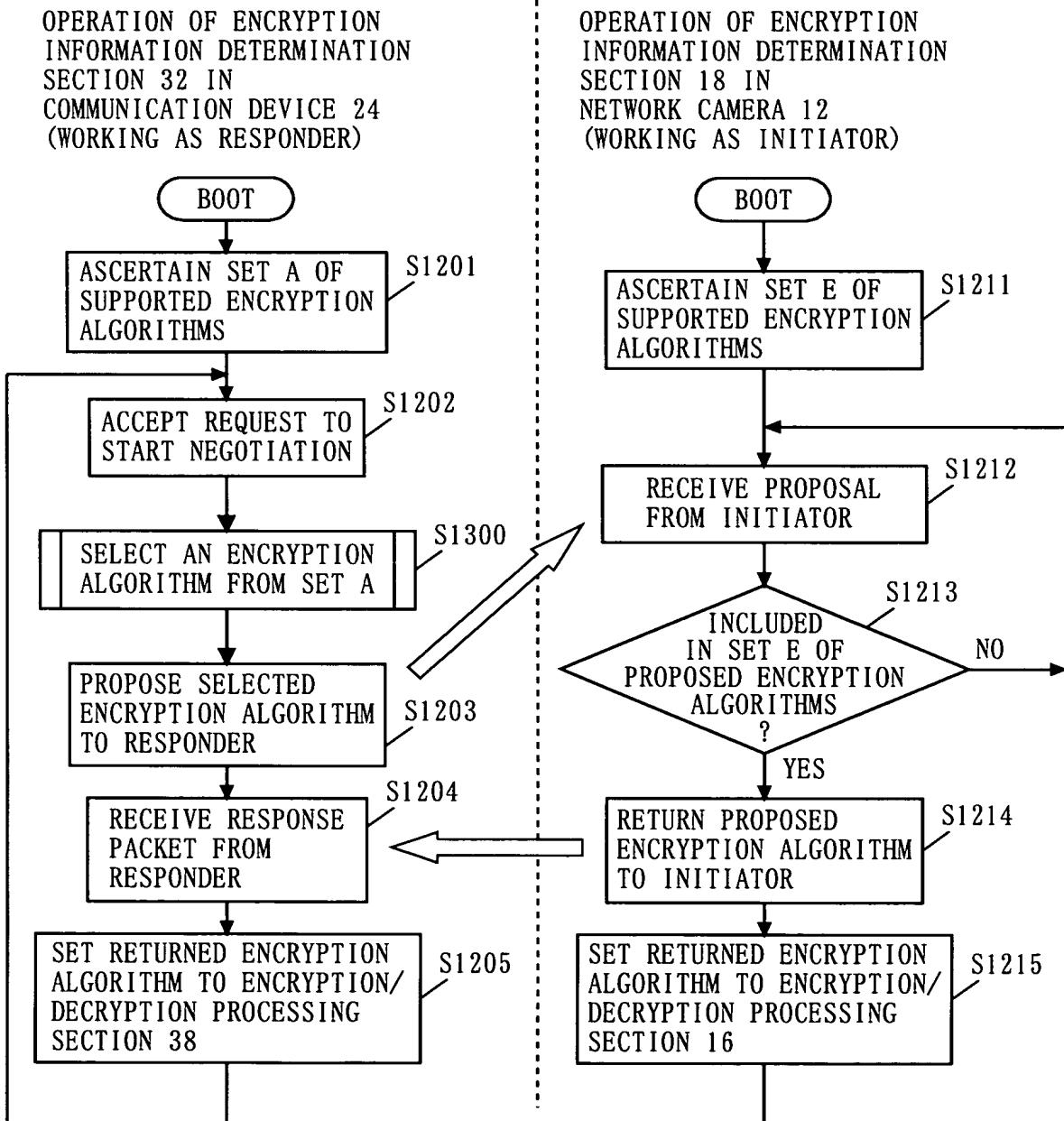
F I G. 1 0



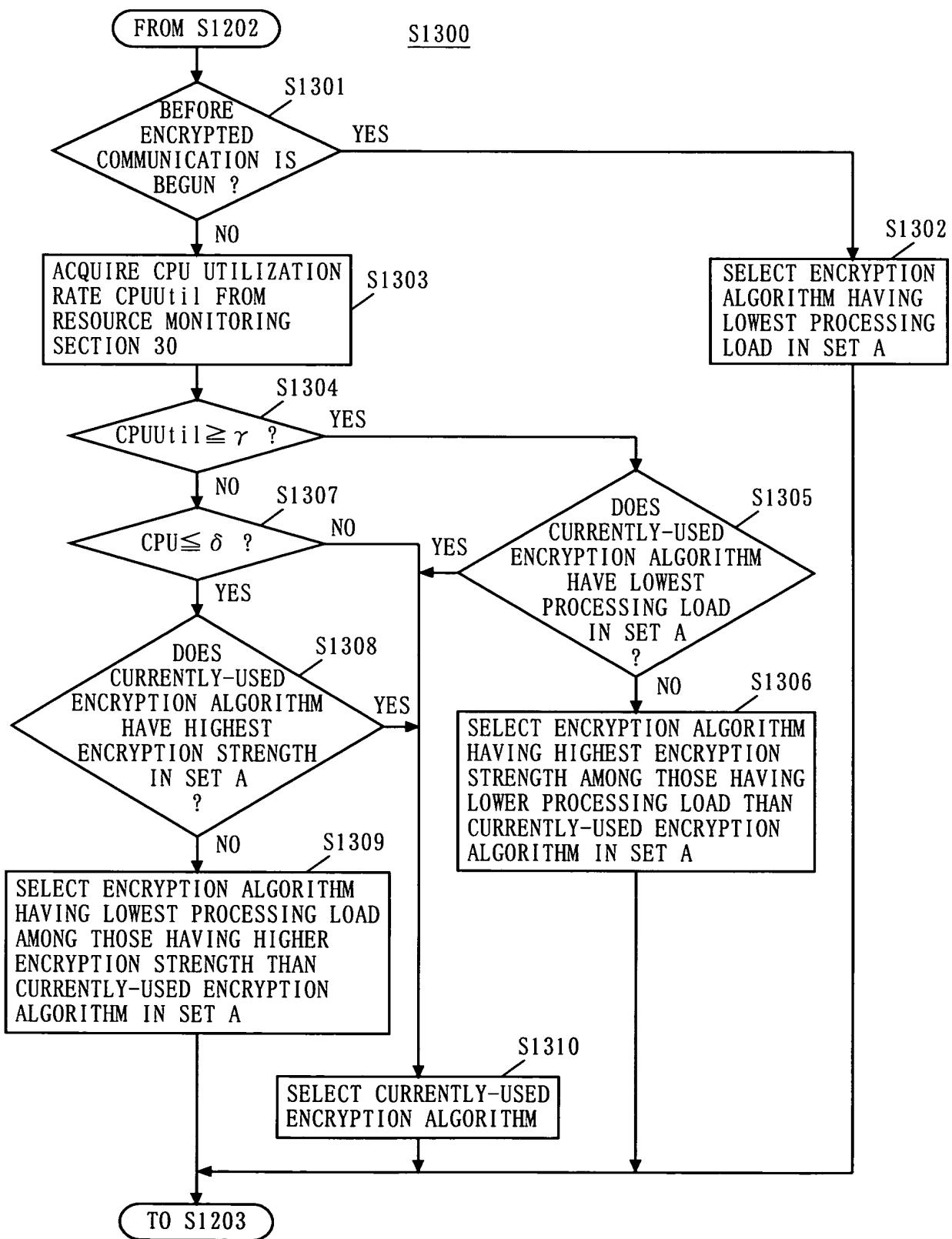
F I G. 11



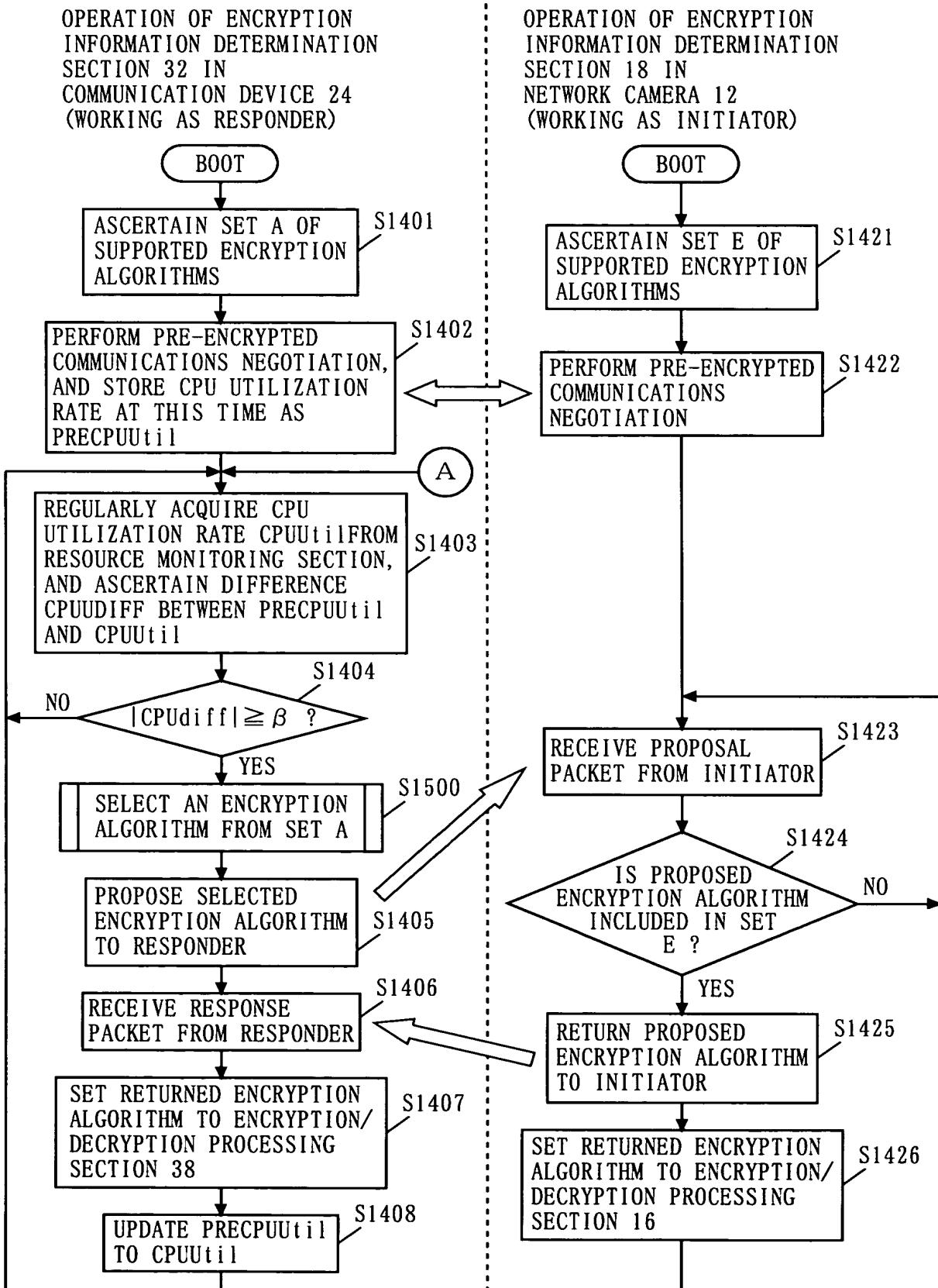
F I G. 1 2



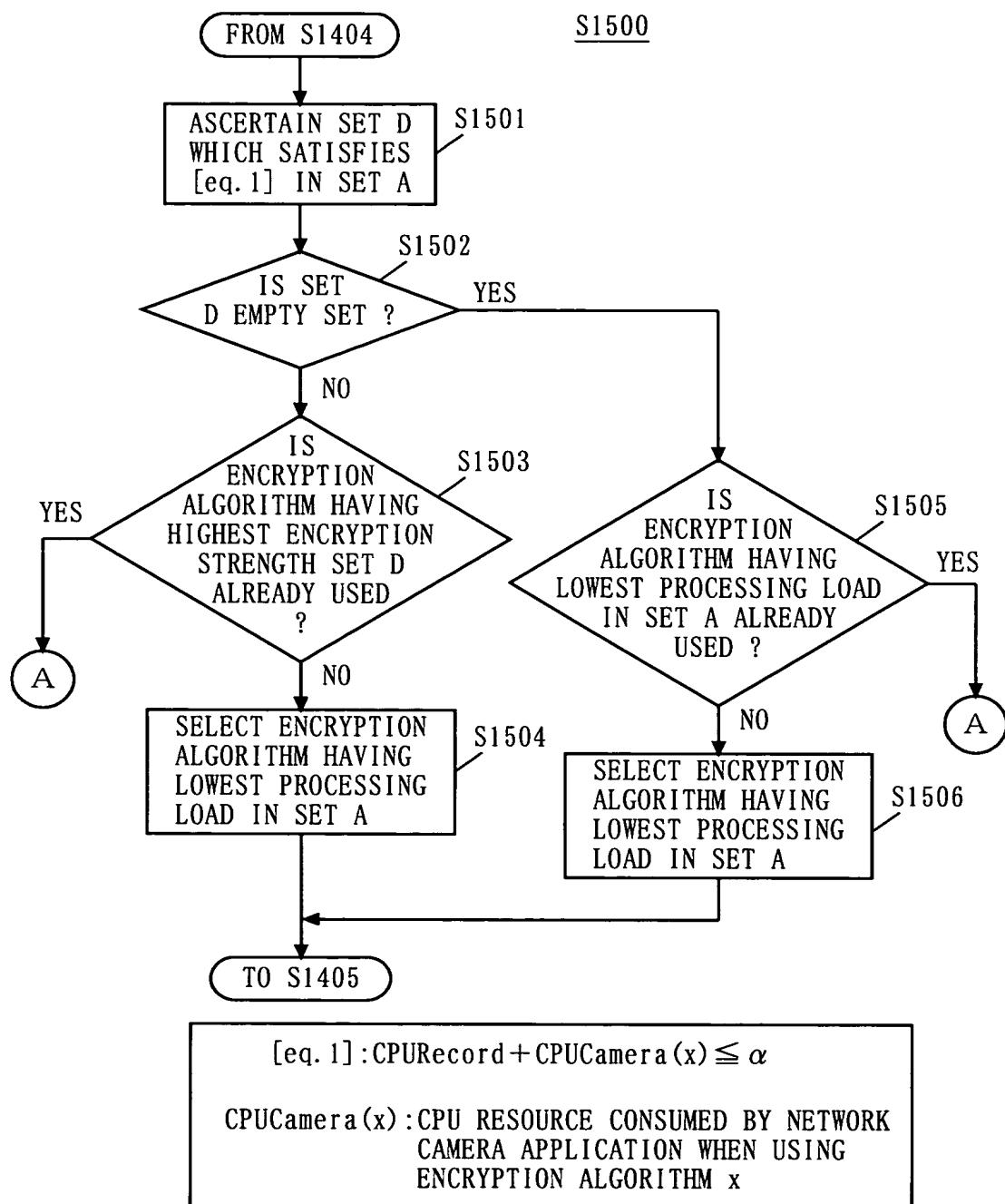
F I G. 13



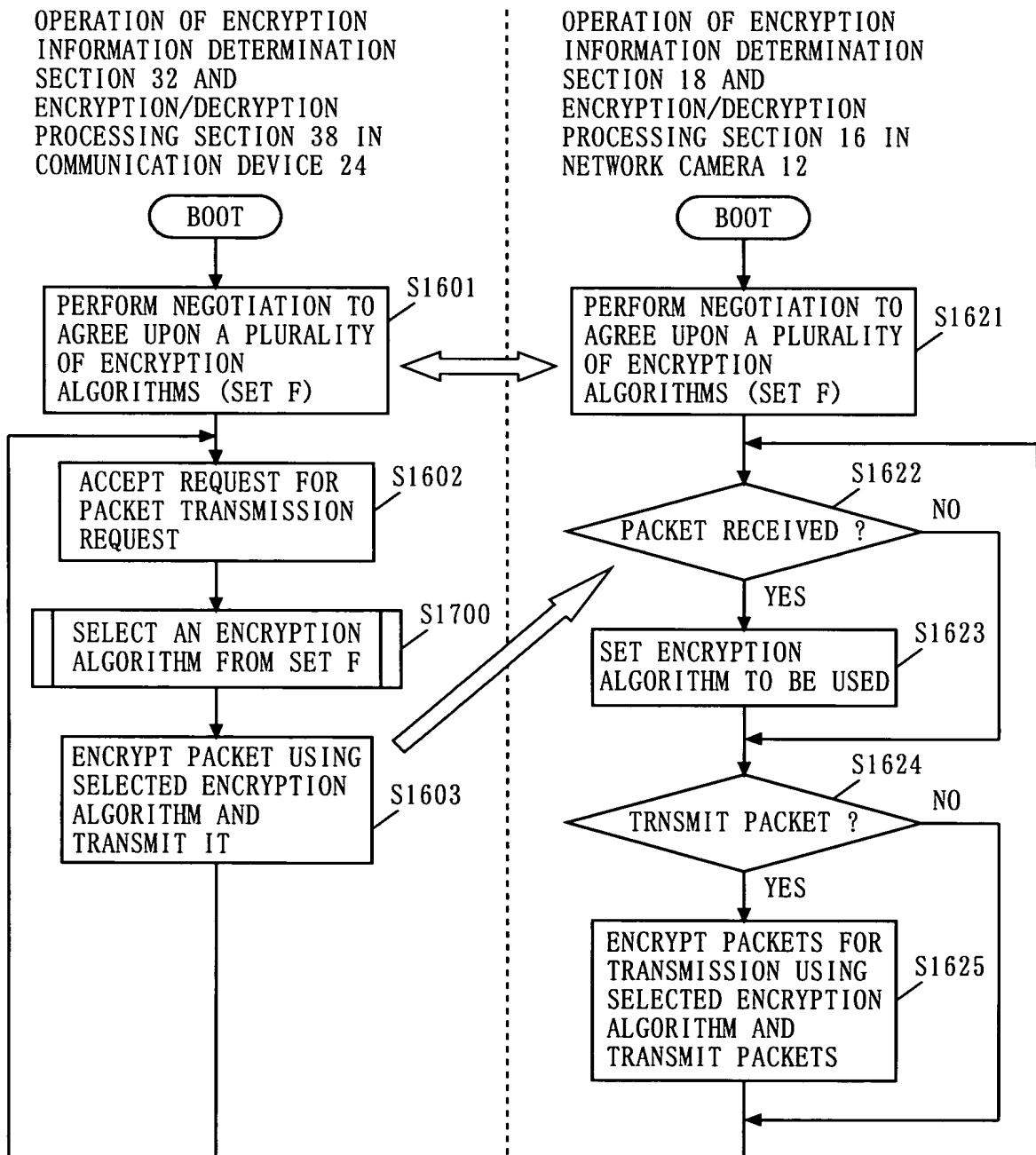
F I G. 1 4



F I G. 1 5



F I G. 1 6



F I G. 17

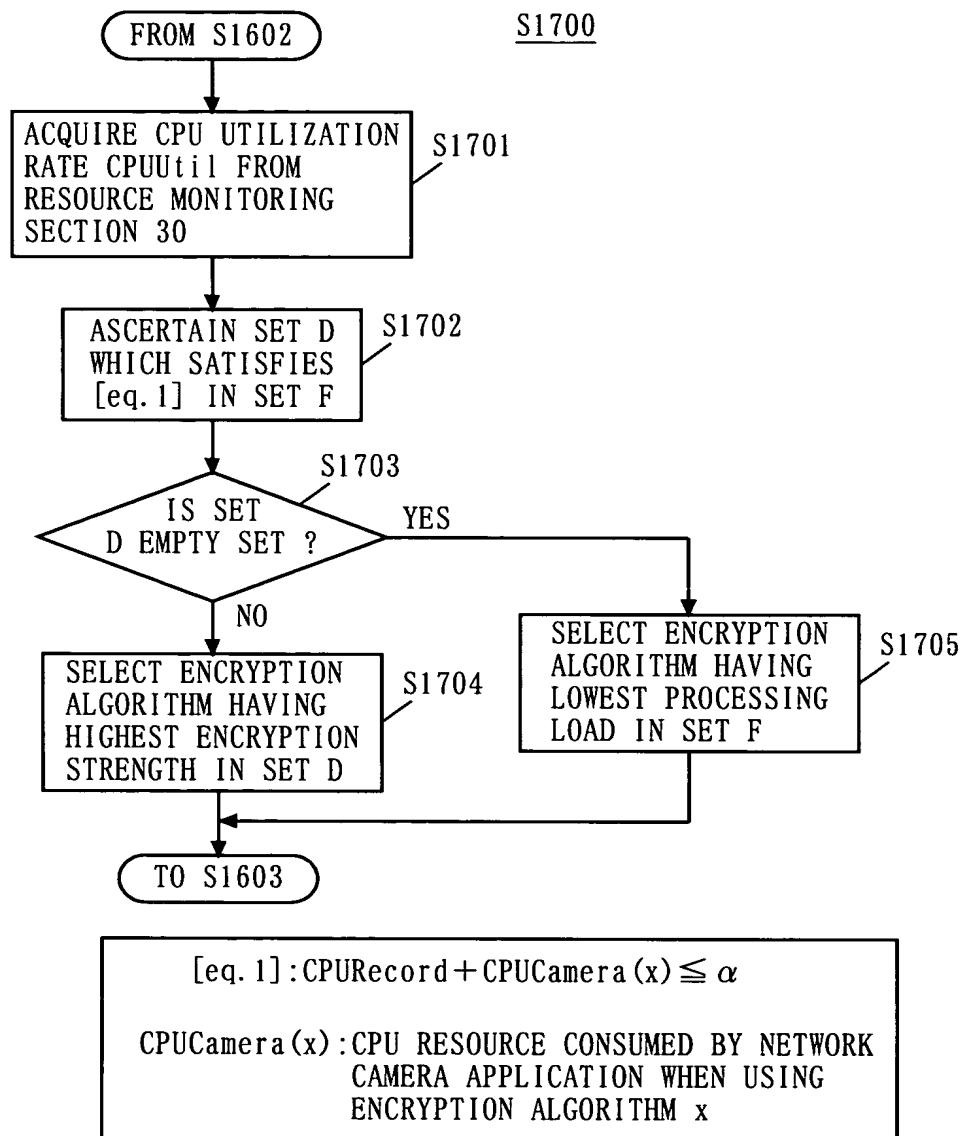


FIG. 18

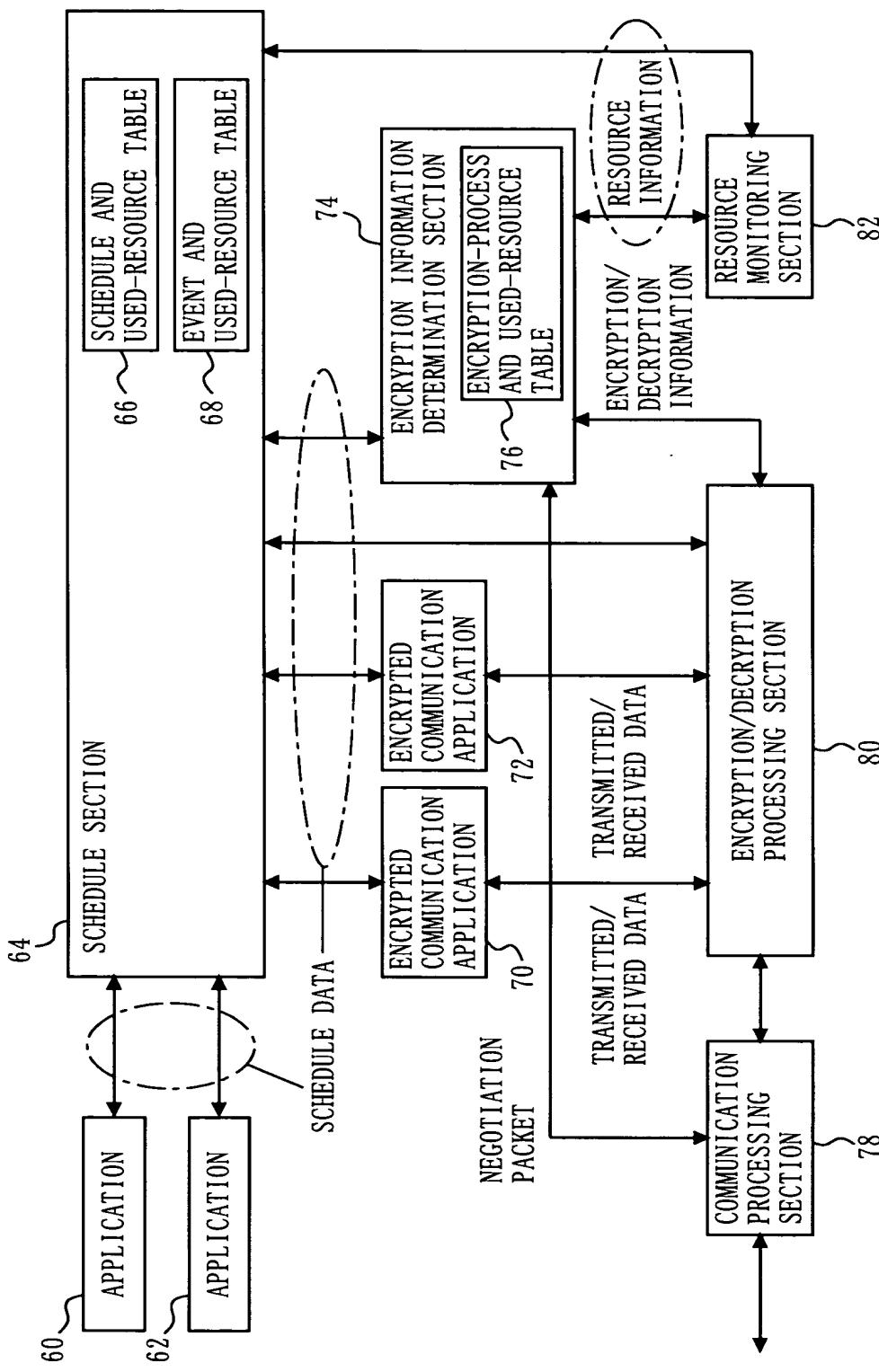


FIG. 19

SCHEDULE AND USED-RESOURCE TABLE IN SCHEDULE SECTION

TASK	BELONGS TO APPLICATION	START TIME	END TIME	AVERAGE USED CPU RESOURCE	AVERAGE USED MEMORY RESOURCE	AVERAGE DATA TRANSFER AMOUNT	ENCRYPTED COMMUNICATION	NECESSARY ENCRYPTION STRENGTH
TASK a	A	2002/11/1 12:00	2002/11/1 13:00	200MIPS	50MB	0Mbps	NO	—
TASK b	B	2002/11/1 14:45	— (UNKNOWN)	50MIPS	20MB	1Mbps	YES	THIRD OR HIGHER
TASK c	A	2002/11/1 12:30	2002/11/1 13:30	100MIPS	20MB	0Mbps	NO	—

("AVERAGE DATA TRANSFER AMOUNT" MEANS AVERAGE DATA TRANSFER AMOUNT FOR ENCRYPTED COMMUNICATIONS)

F I G. 2 0

ENCRYPTION-PROCESS AND USED-RESOURCE TABLE IN ENCRYPTION
INFORMATION DETERMINATION SECTION

ENCRYPTION ALGORITHM	AVERAGE USED CPU RESOURCE (MIPS/Mbps)	AVERAGE USED MEMORY RESOURCE (MB)	ORDER OF ENCRYPTION STRENGTH
DES-CBC	100	13	2
3DES-CBC	300	20	1

FIG. 21

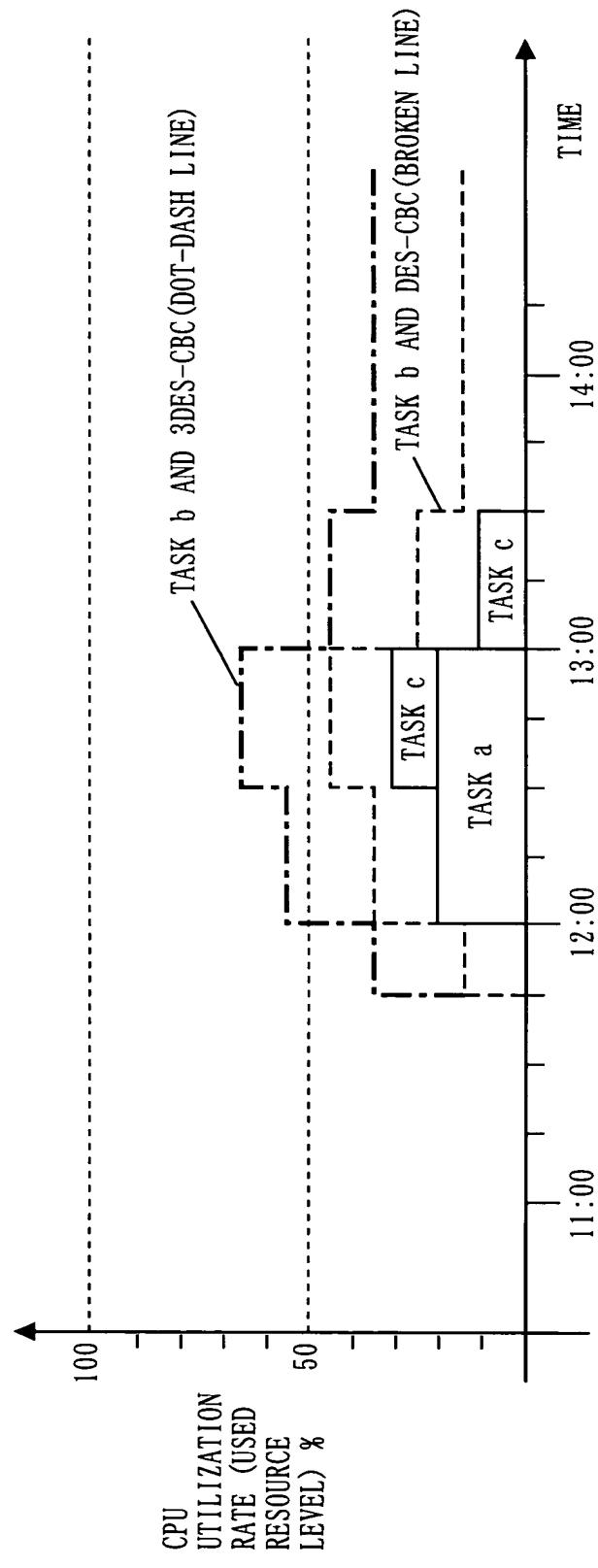


FIG. 22 A

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC)

EVENT TIME	TASK b		ENCRYPTION ALGORITHM		TASK a		TASK c		TOTAL USED RESOURCE
	OPERATING STATE	USED RESOURCE	ALGORITHM NAME	USED RESOURCE	OPERATING STATE	USED RESOURCE	OPERATING STATE	USED RESOURCE	
2002/11/1 11:45	ACTIVE	50MIPS	DES-CBC	100MIPS	INACTIVE		INACTIVE		150MIPS
2002/11/1 12:00	ACTIVE	50MIPS	DES-CBC	100MIPS	ACTIVE	200MIPS	INACTIVE		350MIPS
2002/11/1 12:30	ACTIVE	50MIPS	DES-CBC	100MIPS	ACTIVE	200MIPS	ACTIVE	100MIPS	450MIPS
2002/11/1 13:00	ACTIVE	50MIPS	DES-CBC	100MIPS	INACTIVE		ACTIVE	100MIPS	250MIPS
2002/11/1 13:30	ACTIVE	50MIPS	DES-CBC	100MIPS	INACTIVE		INACTIVE		150MIPS

("USED RESOURCE" MEANS AVERAGE USED CPU RESOURCE)

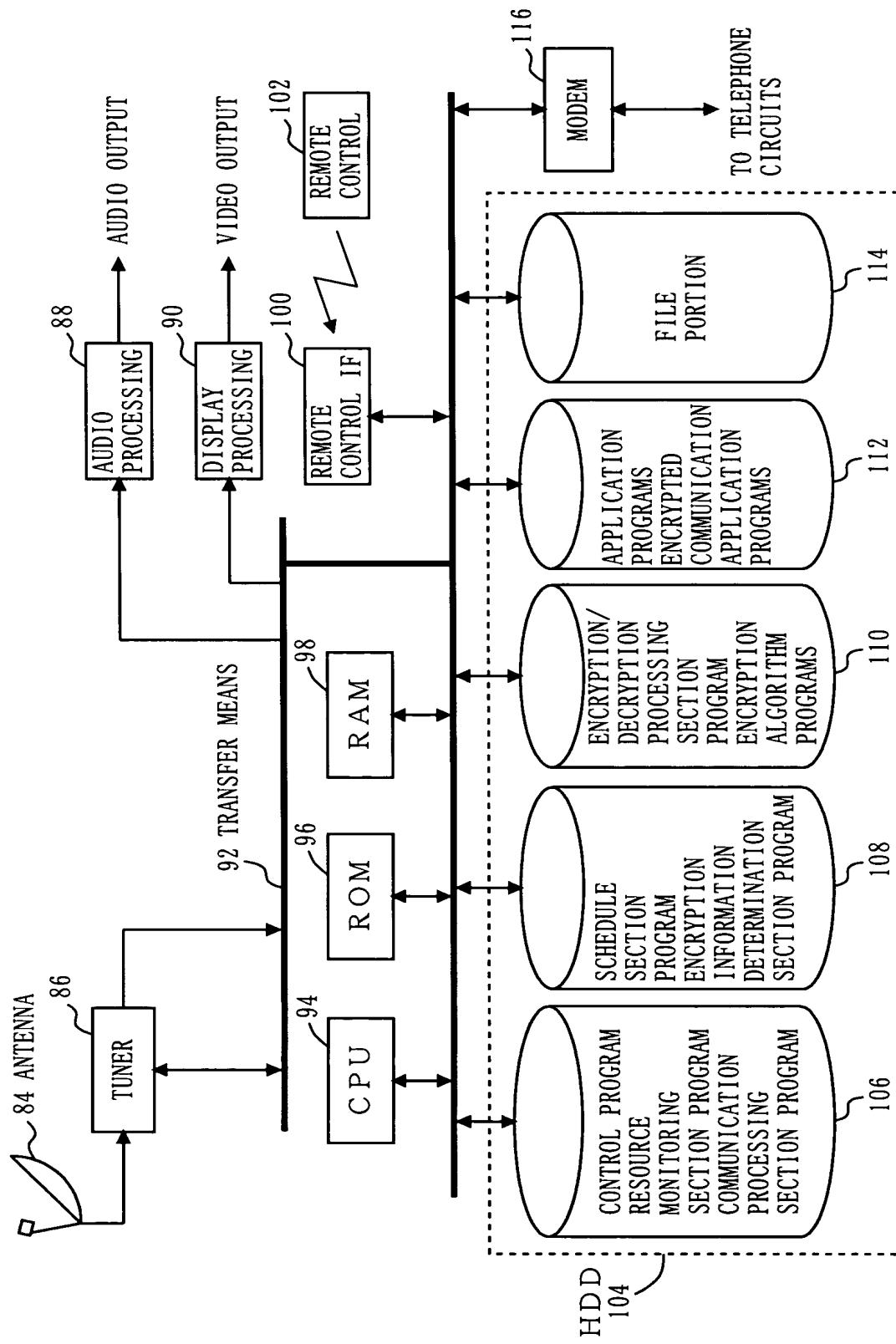
FIG. 22 B

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (3DES-CBC)

EVENT TIME	TASK b		ENCRYPTION ALGORITHM		TASK a		TASK c		TOTAL USED RESOURCE
	OPERATING STATE	USED RESOURCE	ALGORITHM NAME	USED RESOURCE	OPERATING STATE	USED RESOURCE	OPERATING STATE	USED RESOURCE	
2002/11/1 11:45	ACTIVE	50MIPS	3DES-CBC	300MIPS	INACTIVE		INACTIVE		350MIPS
2002/11/1 12:00	ACTIVE	50MIPS	3DES-CBC	300MIPS	ACTIVE	200MIPS	INACTIVE		550MIPS
2002/11/1 12:30	ACTIVE	50MIPS	3DES-CBC	300MIPS	ACTIVE	200MIPS	ACTIVE	100MIPS	650MIPS
2002/11/1 13:00	ACTIVE	50MIPS	3DES-CBC	300MIPS	INACTIVE		ACTIVE	100MIPS	450MIPS
2002/11/1 13:30	ACTIVE	50MIPS	3DES-CBC	300MIPS	INACTIVE		INACTIVE		350MIPS

("USED RESOURCE" MEANS AVERAGE USED CPU RESOURCE)

FIG. 23



F I G. 2 4

ENCRYPTION-PROCESS AND USED-RESOURCE TABLE IN ENCRYPTION
INFORMATION DETERMINATION SECTION

ENCRYPTION ALGORITHM	AVERAGE USED CPU RESOURCE (MIPS/Mbps)	NUMBER OF PREPROCESS INSTRUCTIONS (MI)	ORDER OF ENCRYPTION STRENGTH
DES-CBC	100	100	2
3DES-CBC	300	300	1

FIG. 25

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	TASK/ RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	USED ENCRYPTION ALGORITHM
11:45	b 50			D 100	150	3D 300	350	3D
12:00	b 50	a 200		D 100	350	3D 300	550	D
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	D
13:00	b 50	c 100		D 100	250	3D 300	450	3D
13:30	b 50			D 100	150	3D 300	350	3D

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS) ; "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC)

FIG. 26

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	WHEN USING ALGORITHM D FOR TASK b		WHEN USING ALGORITHM 3D FOR TASK b		USED ENCRYPTION ALGORITHM
			RESOURCE	TOTAL RESOURCE	RESOURCE	TOTAL RESOURCE	
11:45	b 50		100	150	300	350	3D
12:00	b 50	a 200	100	350	300	550	D
12:30	b 50	a 200	c 100	100	450	300	D
13:00	b 50	c 100		100	250	300	450
13:30	b 50			100	150	300	3D

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS); "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC)

FIG. 27

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	USED ENCRYPTION ALGORITHM	PREPROCESS ENCRYPTION ALGORITHM	Mt 1	3D
11:42										
11:45	b 50		D 100	150	3D 300	350	3D			
11:58	SAME AS ABOVE		SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	SAME AS ABOVE	3D	Mt 2	D	
12:00	b 50	a 200	D 100	350	3D 300	550	D			
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	D		
12:56	SAME AS ABOVE	D	Mt 3	3D						
13:00	b 50	c 100		D 100	250	3D 300	450	3D		
13:30	b 50			D 100	150	3D 300	350	3D		

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS); "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC)

FIG. 28

EVENT AND USED-RESOURCE TABLE IN SCHEDULE SECTION (DES-CBC, 3DES-CBC, AES)

EVENT TIME	TASK/ RESOURCE	TASK/ RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	CODE/ RESOURCE	TOTAL RESOURCE	USED ENCRYPTION ALGORITHM	PREPROCESS ENCRYPTION ALGORITHM
11:43										
11:45	b 50		D 100	150	3D 300	350	A 200	250	A	
12:00	b 50	a 200	D 100	350	3D 300	550	A 200	450	A	
12:29	SAME AS ABOVE	A	Mt 2							
12:30	b 50	a 200	c 100	D 100	450	3D 300	650	A 200	550	D
12:58	SAME AS ABOVE	D	Mt 3							
13:00	b 50	c 100		D 100	250	3D 300	450	A 200	350	A
13:30	b 50			D 100	150	3D 300	350	A 200	250	A

("RESOURCE" MEANS AVERAGE USED CPU RESOURCE (MIPS); "D" MEANS DES-CBS; "3D" MEANS 3DES-CBC; "A" MEANS AES)

F I G. 29

ENCRYPTION-PROCESS AND USED-RESOURCE TABLE IN ENCRYPTION
INFORMATION DETERMINATION SECTION

ENCRYPTION ALGORITHM	AVERAGE USED CPU RESOURCE (MIPS/Mbps)	AVERAGE USED MEMORY RESOURCE (MB)	ORDER OF ENCRYPTION STRENGTH
DES-CBC	100	13	3
3DES-CBC	300	20	2
AES	200	16	1

F I G. 3 0

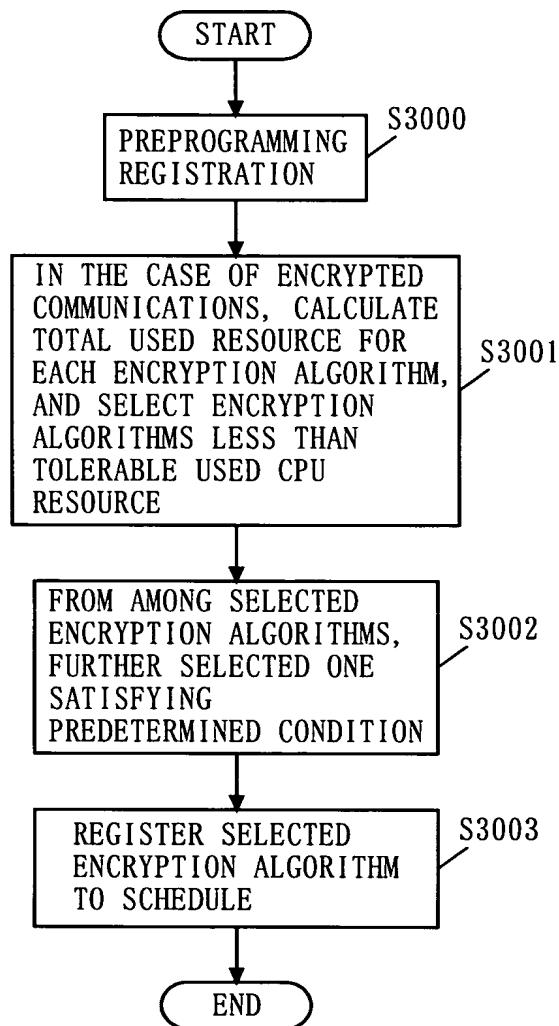


FIG. 31

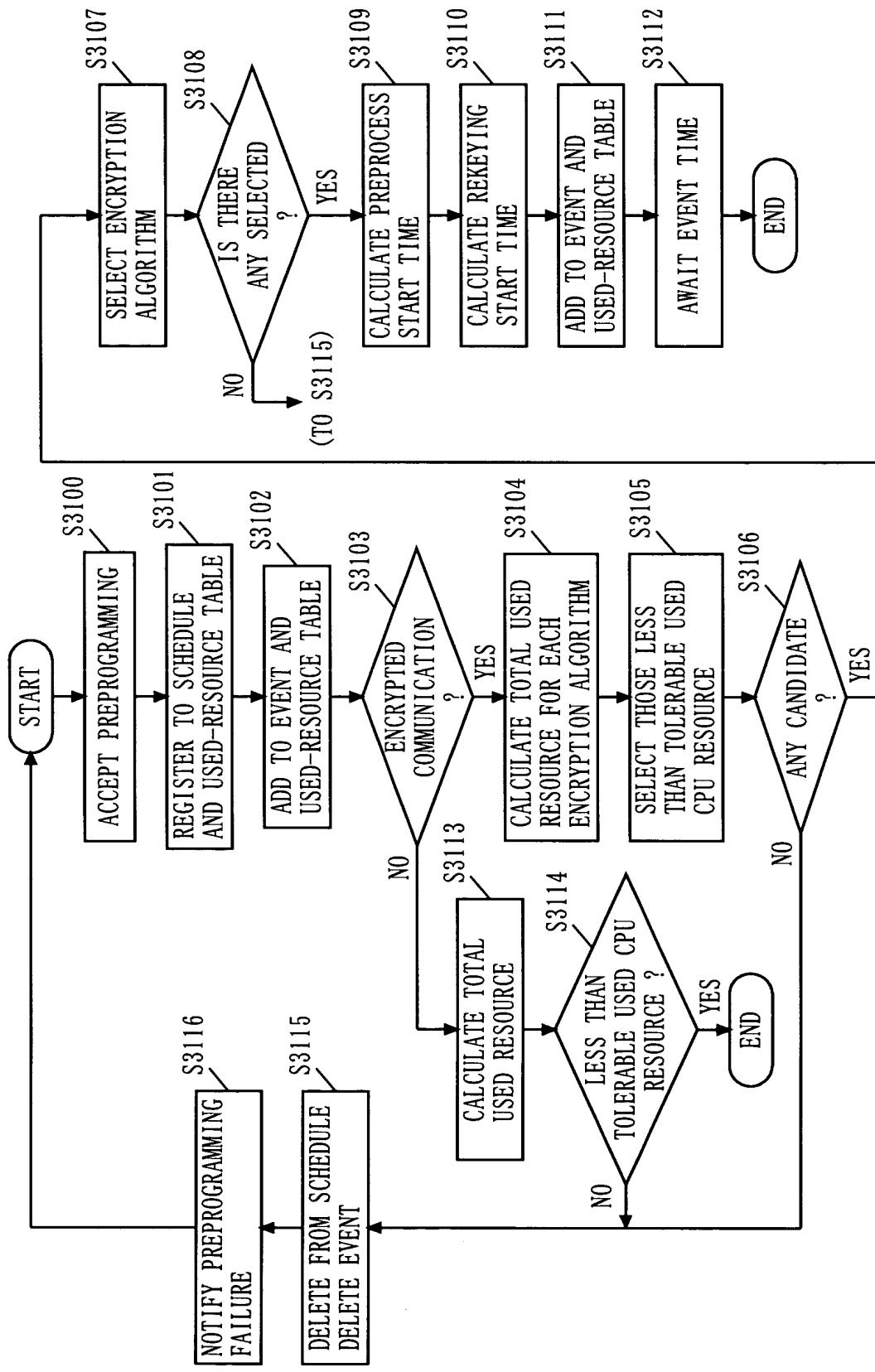


FIG. 32

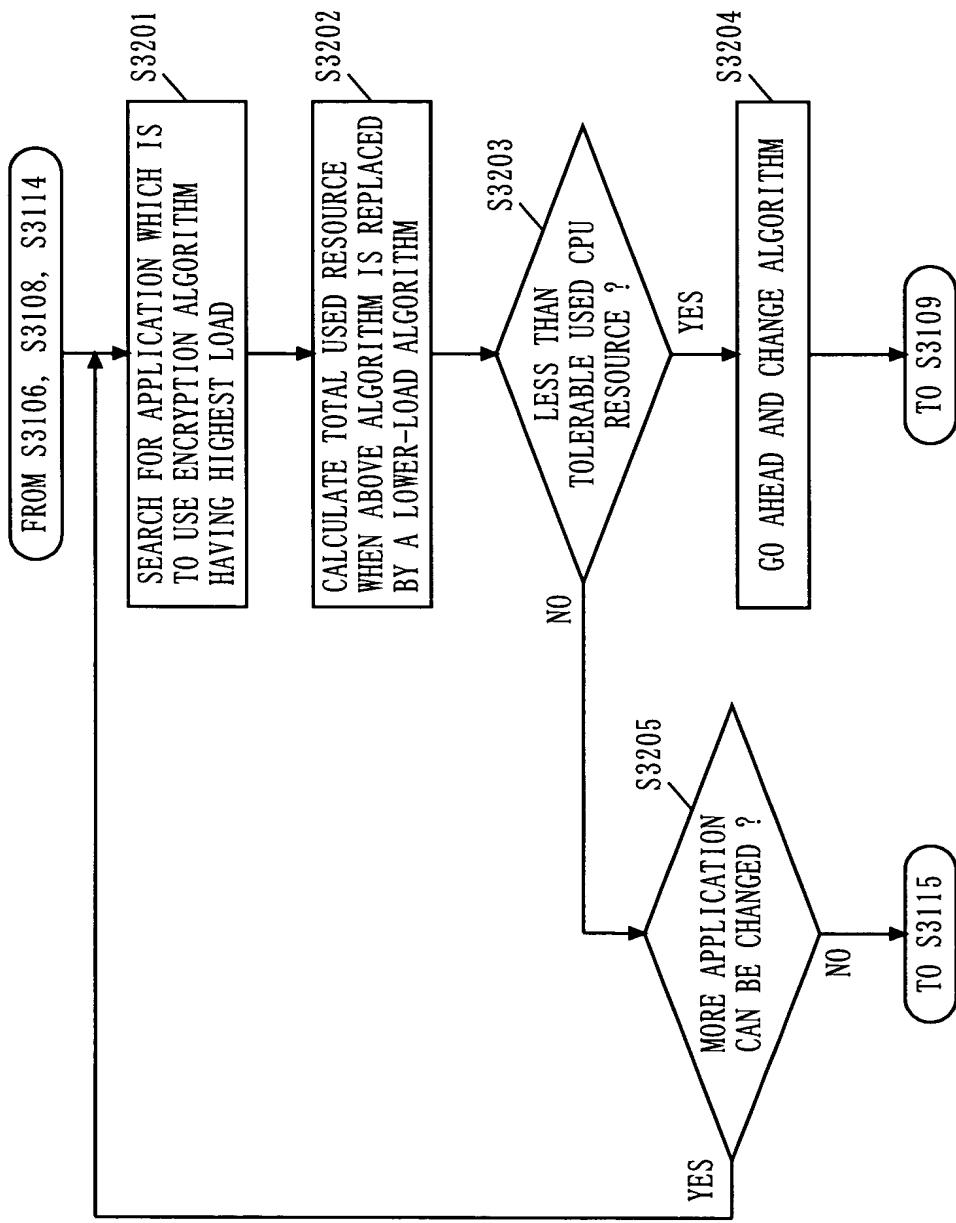


FIG. 33

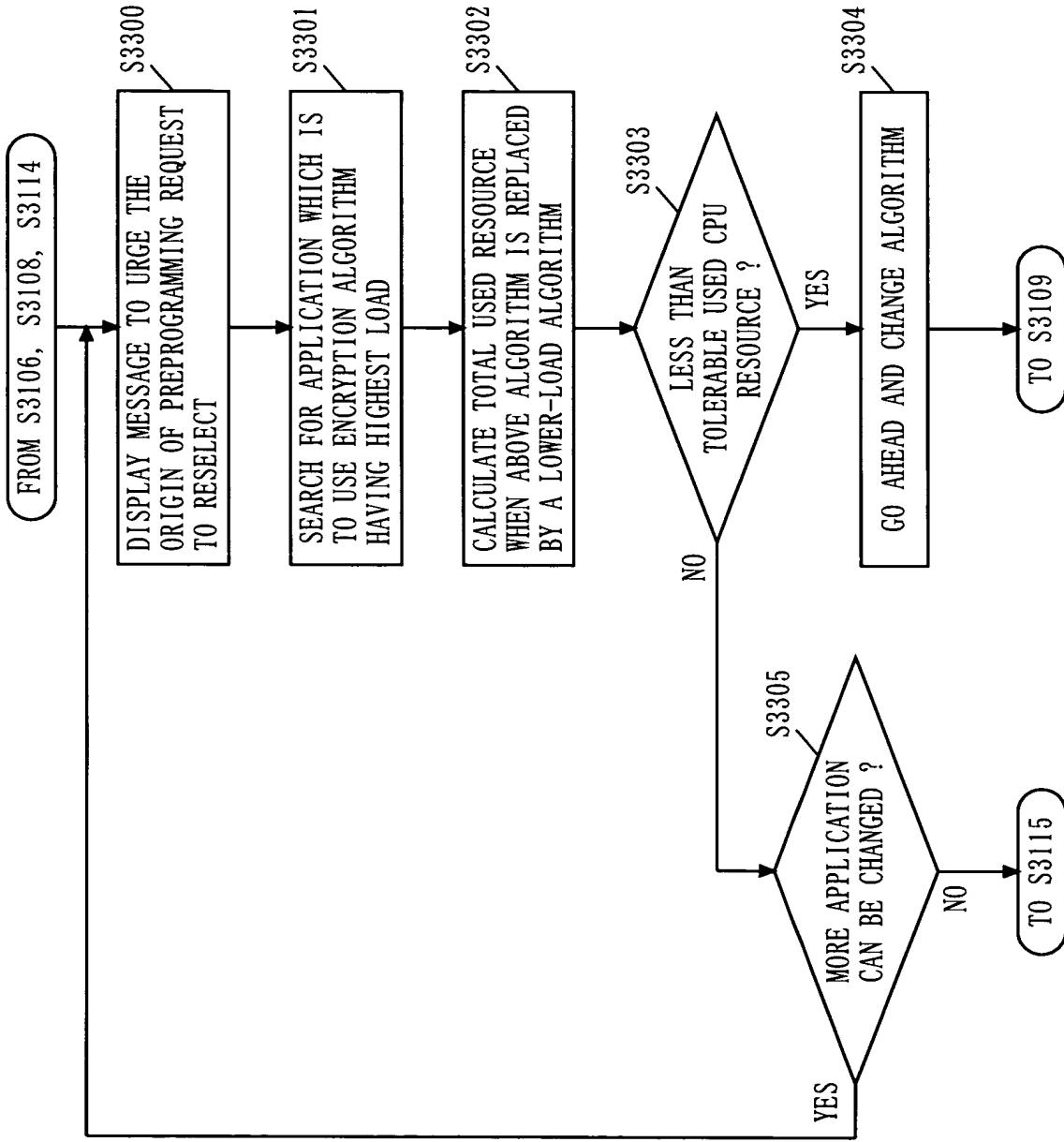


FIG. 34

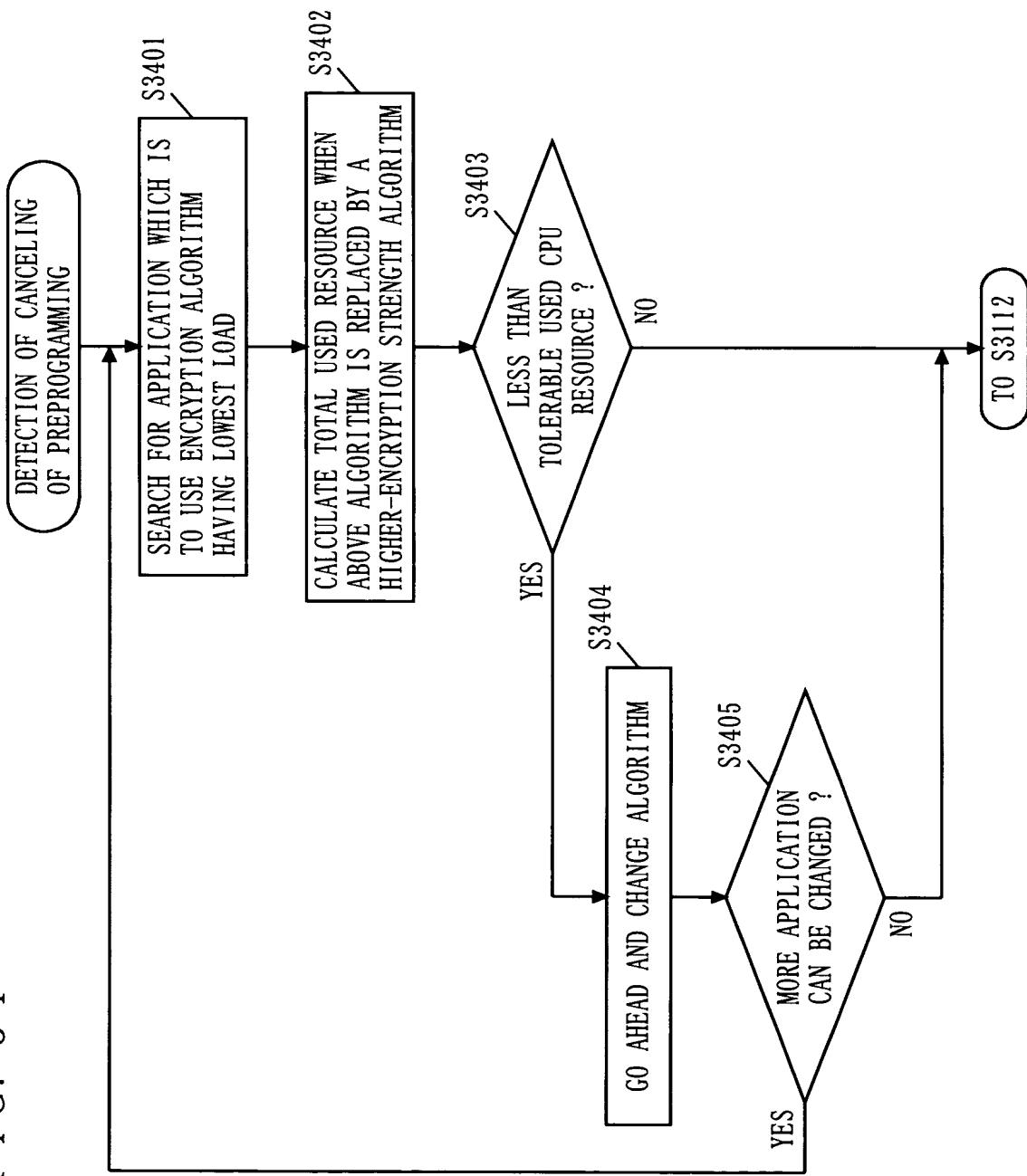


FIG. 35

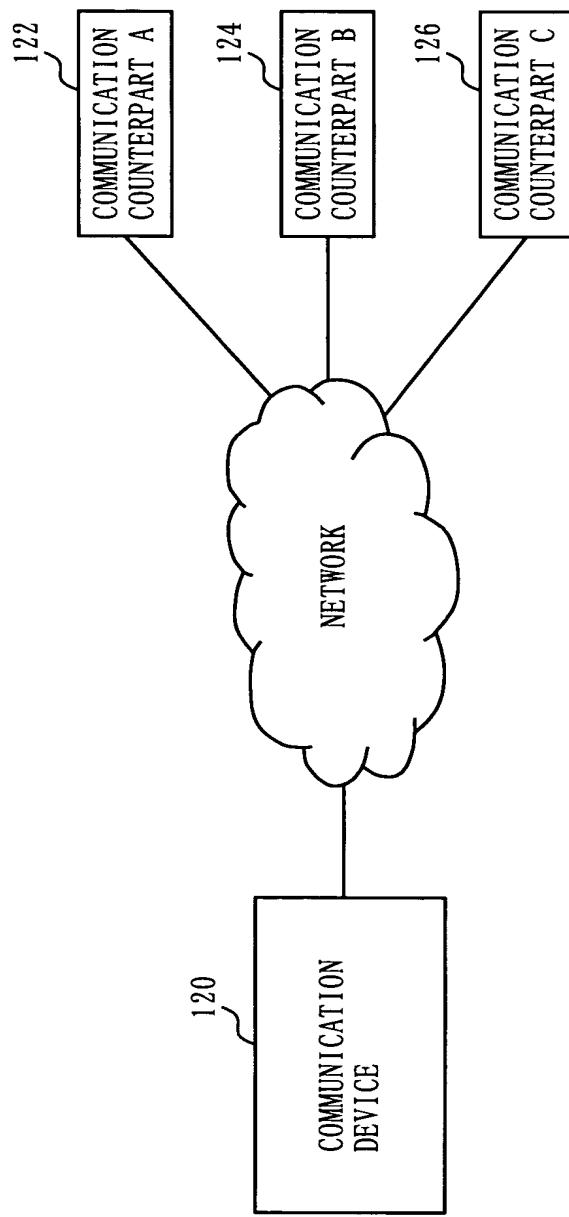
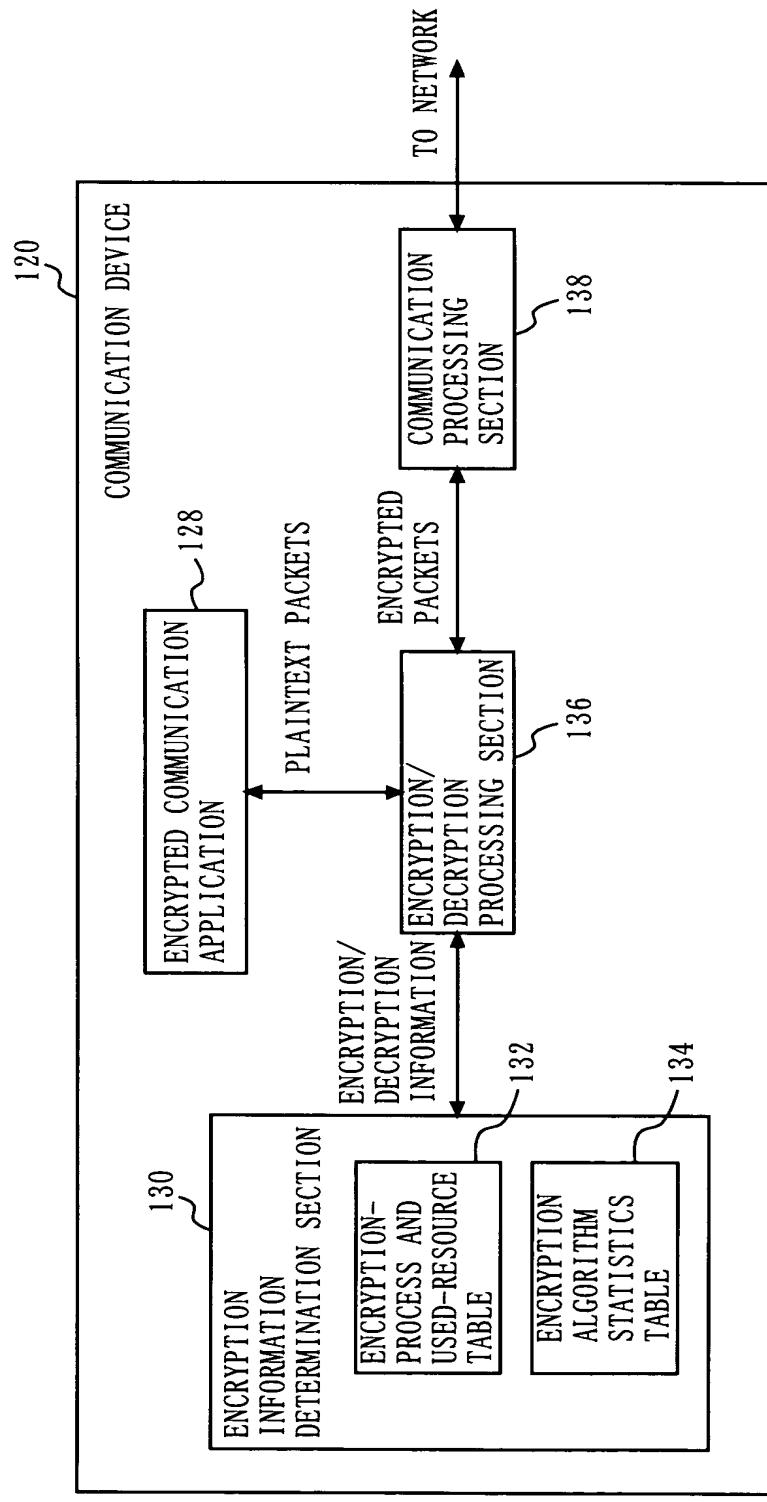


FIG. 36



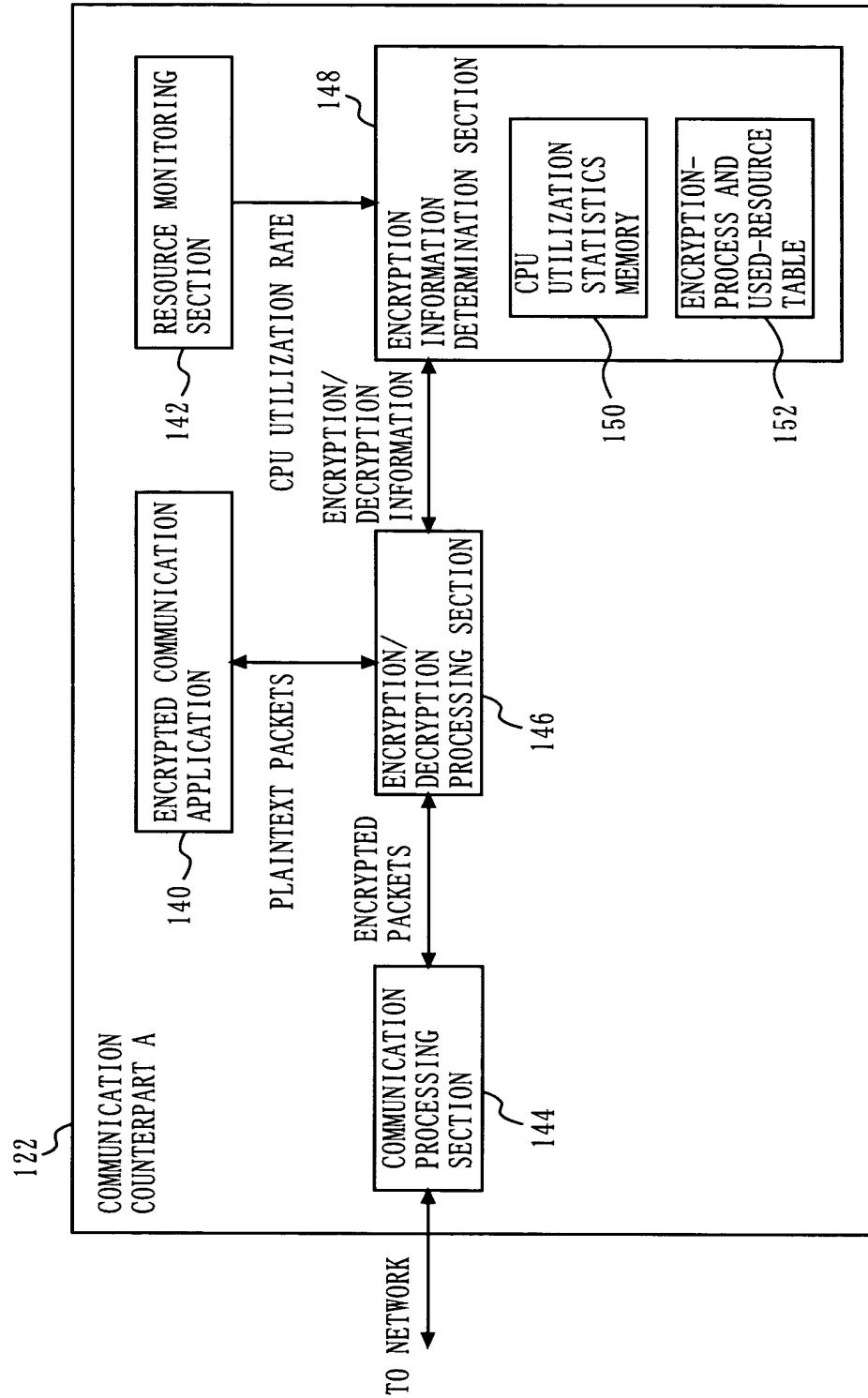
F I G. 37

ALGORITHM	CALCULATION AMOUNT	CALCULATION INDEX (ORDER)	ENCRYPTION AMOUNT (ORDER)	STRENGTH
DES-CBC	100	1		3
3DES-CBC	300	3		2
AES-CBC	200	2		1

F I G. 38

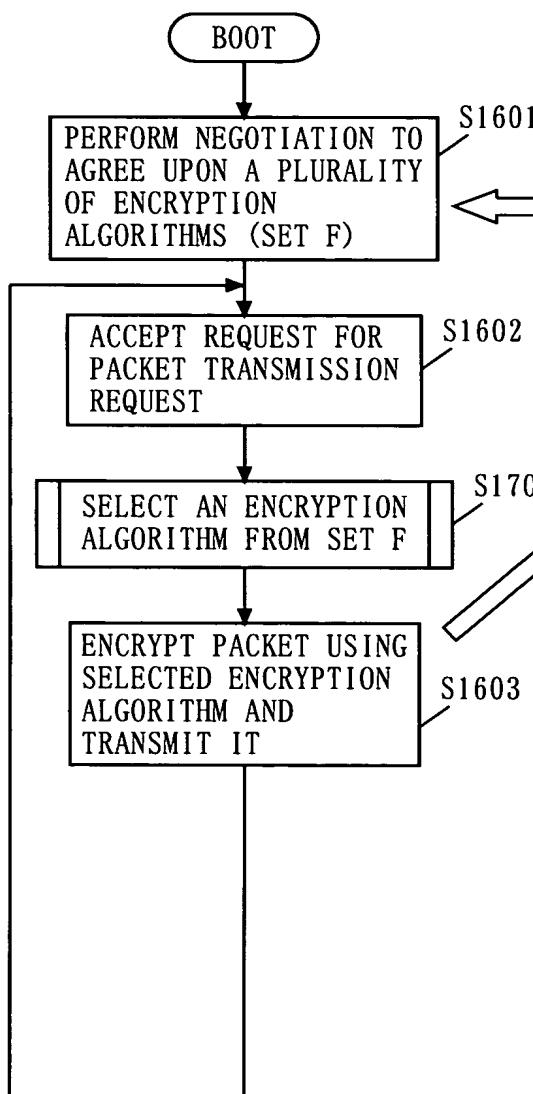
COMMUNICATION COUNTERPART	Last	FREQUENCY		
		DES	3DES	AES
COMMUNICATION COUNTERPART A	3DES-CBC	17	3	*
COMMUNICATION COUNTERPART B	3DES-CBC	*	13	7
COMMUNICATION COUNTERPART C	AES-CBC	*	5	15

FIG. 39



F I G. 4 0

OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 148 AND ENCRYPTION/DECRYPTION PROCESSING SECTION 146 IN COMMUNICATION COUNTERPART 122



OPERATION OF ENCRYPTION INFORMATION DETERMINATION SECTION 130 AND ENCRYPTION/DECRYPTION PROCESSING SECTION 136 IN COMMUNICATION DEVICE 120

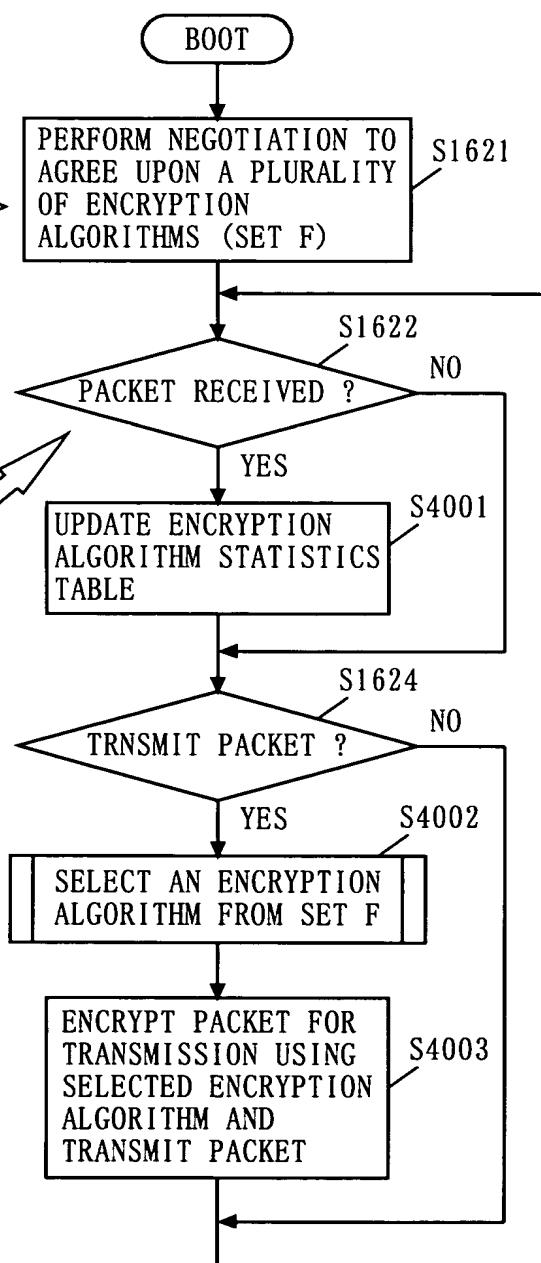


FIG. 41

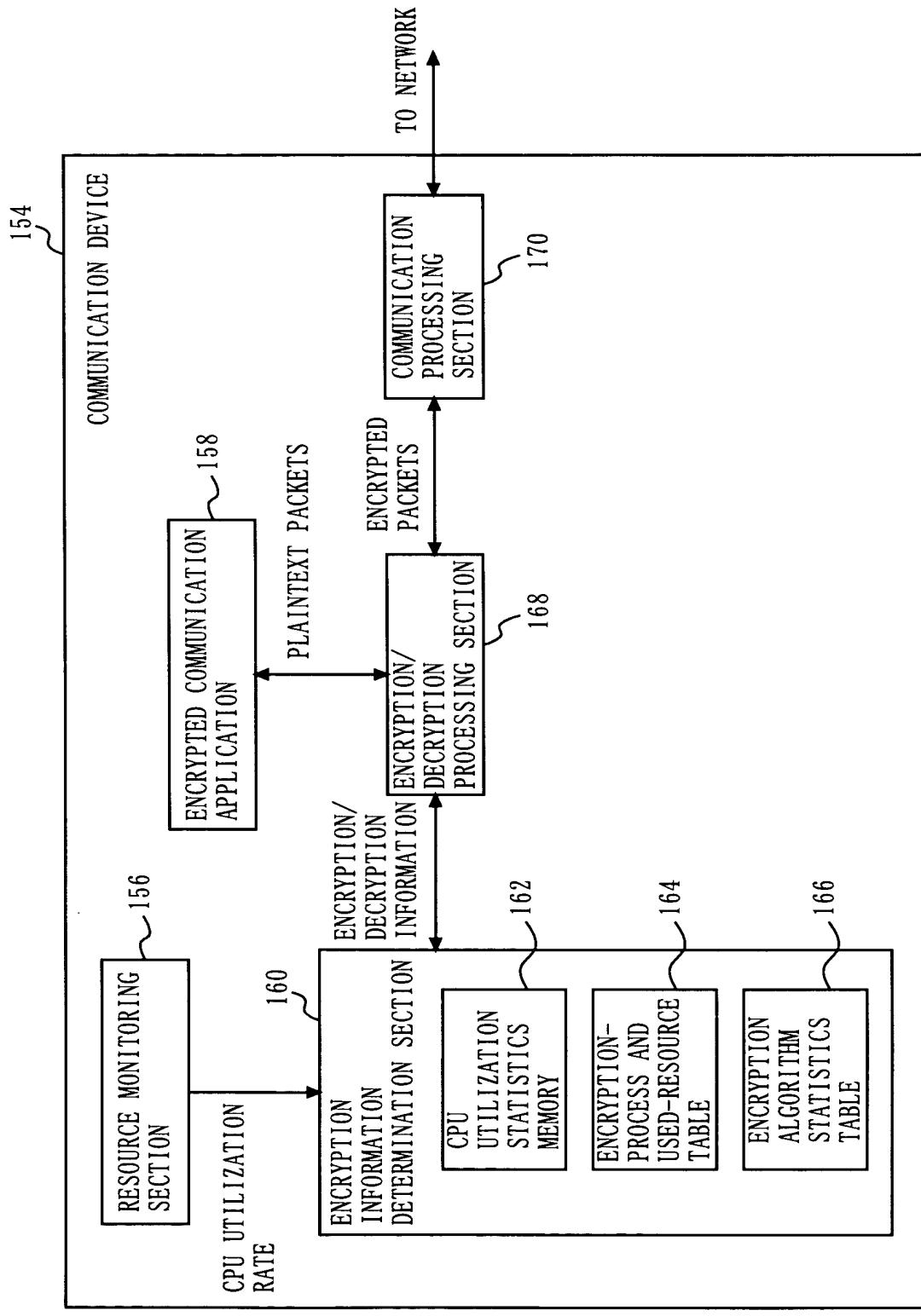


FIG. 42 PRIOR ART

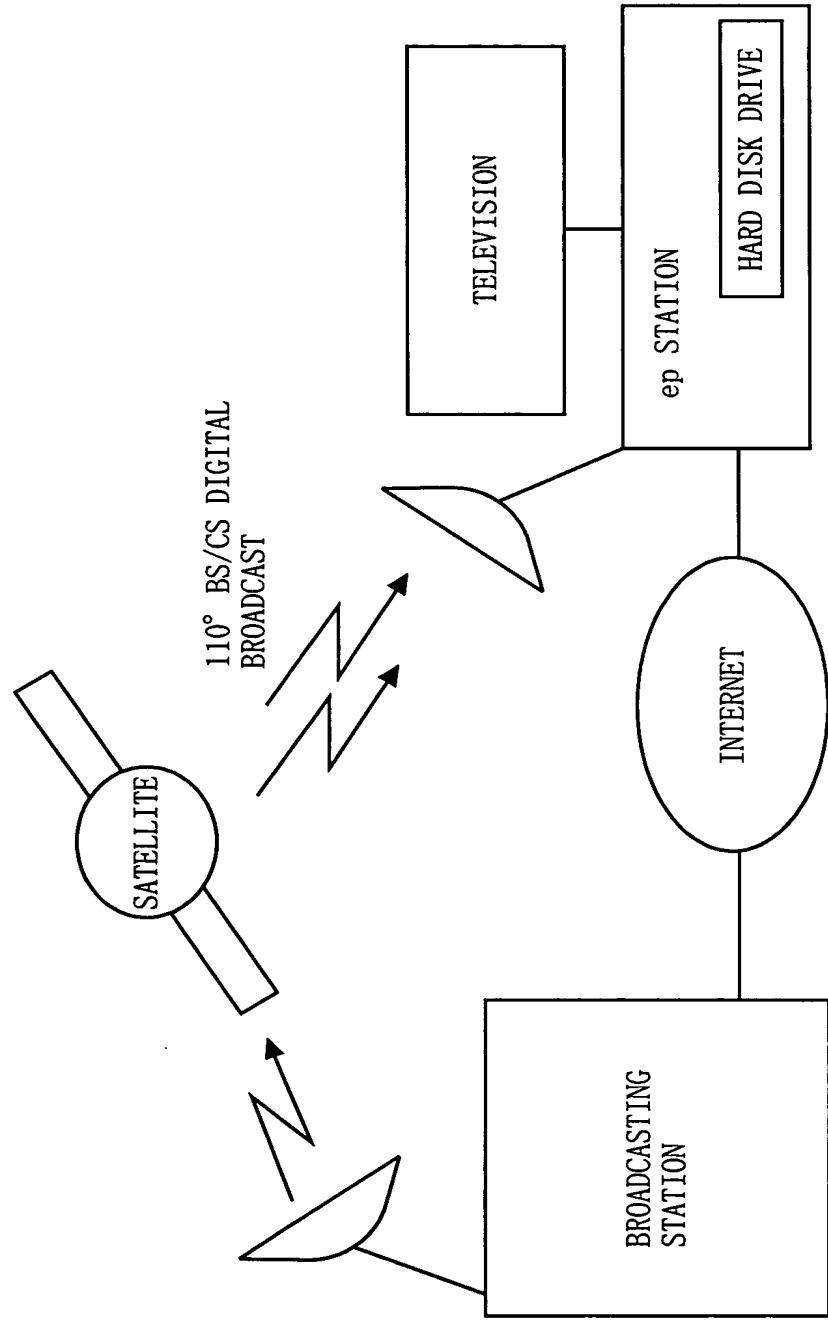


FIG. 43 PRIOR ART

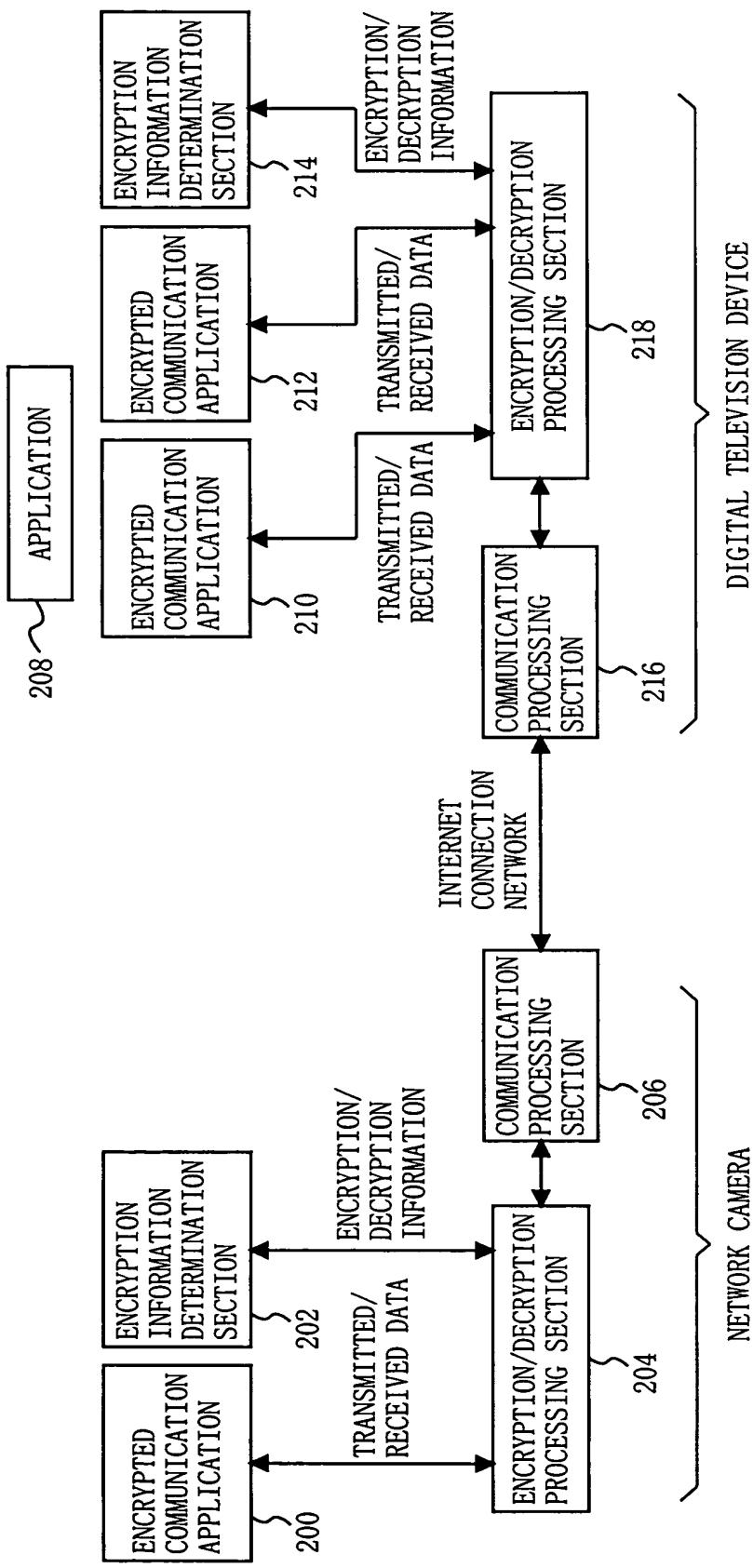


FIG. 44 PRIOR ART

